(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－22844
（P2001－22844A）
(43)公開日　平成13年１月26日(2001.1.26)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	17/60		Ｇ０６Ｆ 15/21	３３０	５Ｂ０４９
	13/00	３５４	13/00	３５４Ｄ	５Ｂ０８９
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ 1/00	６４０Ｂ	５Ｄ０４４
				６４０Ｚ	５Ｊ１０４
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ 20/10	Ｈ	９Ａ００１

審査請求　未請求　請求項の数84　ＯＬ　（全 88 頁）　最終頁に続く

(21)出願番号　特願平11－193561

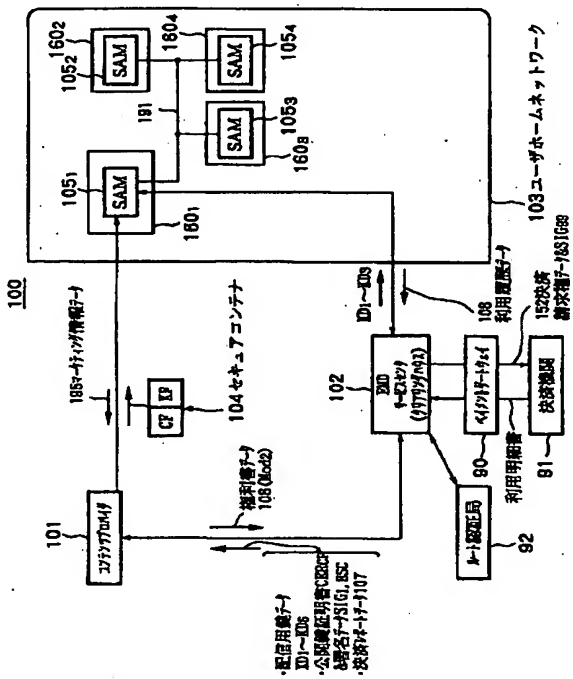
(22)出願日　平成11年７月７日(1999.7.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　野中　聡
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　江崎　正
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100094053
弁理士　佐藤　隆久

最終頁に続く

(54)【発明の名称】　データ提供システムおよびその方法、管理装置およびデータ処理装置

(57)【要約】
【課題】　データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。
【解決手段】　コンテンツプロバイダ１０１は、コンテンツデータとその権利書データとを格納したセキュアコンテナ１０４をＳＡＭ１０５$_1$に配給し、ＳＡＭ１０５$_1$は、配給を受けた権利書データに基づいて配給を受けたコンテンツデータの購入・利用形態を決定し、当該決定した購入・利用形態の履歴を示す利用履歴データ１０８をＥＭＤサービスセンタ１０２に送信し、ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づいて、ユーザが支払った金銭をコンテンツプロバイダ１０１の権利者に分配するための処理を行う。



1

【特許請求の範囲】

【請求項１】データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行うデータ提供システム。

【請求項２】前記データ提供装置は、所定の鍵データを用いて前記コンテンツデータを暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記鍵データを用いて、前記受信したコンテンツデータを復号し、

前記管理装置は、前記鍵データを管理する請求項１に記載のデータ提供システム。

【請求項３】前記データ提供装置は、所定の鍵データを生成し、当該生成した鍵データを前記管理装置に登録し、

前記管理装置は、前記登録された前記鍵データを管理し、前記データ処理装置において、前記コンテンツデータの購入処理が行われたときに、対応する前記鍵データを前記データ処理装置に送信し、

前記データ処理装置は、受信した前記鍵データを用いて、前記受信したコンテンツデータを復号する請求項１に記載のデータ提供システム。

【請求項４】前記データ提供装置は、前記鍵データを暗号化し、当該暗号化した鍵データと前記暗号化したコンテンツデータと前記権利書データとを格納したモジュールを前記データ処理装置に配給する請求項２に記載のデータ提供システム。

【請求項５】前記管理装置は、配信用鍵データを管理し、前記配信用鍵データを前記データ提供装置および前記データ処理装置に配給し、

前記データ提供装置は、前記配信された前記配信用鍵データを用いて前記鍵データおよび前記権利書データを暗号化し、

前記データ処理装置は、前記配信された前記配信用鍵データを用いて前記鍵データおよび前記権利書データを復号する請求項４に記載のデータ提供システム。

【請求項６】前記管理装置は、各々所定の有効期限を持つ複数の前記配信用鍵データを、所定の期間分だけ、前

2

記データ提供装置および前記データ処理装置に配給する請求項５に記載のデータ提供システム。

【請求項７】前記データ提供装置は、前記暗号化したコンテンツデータおよび前記権利書データの少なくとも一方に対しての署名データを自らの秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化した前記鍵データ、前記暗号化された前記権利書データおよび前記署名データを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュール内に格納された前記署名データを、前記秘密鍵データに対応する公開鍵データを用いて検証し、

前記管理装置は、前記公開鍵データを管理する請求項４に記載のデータ提供システム。

【請求項８】前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する請求項７に記載のデータ提供システム。

【請求項９】前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する請求項７に記載のデータ提供システム。

【請求項１０】前記管理装置は、前記データ提供装置および前記データ処理装置に、それぞれ配信鍵データを配給し、

前記データ提供装置は、前記権利書データを、前記配信鍵データを用いて暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記配信鍵データを用いて、受信した前記権利書データを復号する請求項１に記載のデータ提供システム。

【請求項１１】前記管理装置は、前記権利書データおよび前記鍵データの少なくとも一方の正当性を認証する請求項２に記載のデータ提供システム。

【請求項１２】前記管理装置は、前記利益分配処理に応じた決済処理を行うことを請求する際に用いられる決済請求権データを生成し、当該決済請求権データに自らの秘密鍵データによる署名データを付加して、前記決済処理を行う装置あるいは前記データ提供装置に送信する請求項１に記載のデータ提供システム。

【請求項１３】前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う請求項１に記載のデータ提供システム。

【請求項１４】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態を決定し、当該決定した購入形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を

制御する請求項１に記載のデータ提供システム。

【請求項１５】前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである請求項１に記載のデータ提供システム。

【請求項１６】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、

前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う管理装置。

【請求項１７】所定の鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、

前記鍵データを管理する請求項１５に記載の管理装置。

【請求項１８】前記権利書データと、前記コンテンツデータを前記暗号化する際に用いる鍵データとの少なくとも一方の正当性を認証する請求項１６に記載の管理装置。

【請求項１９】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信するデータ処理装置。

【請求項２０】前記コンテンツデータが所定の鍵データを用いて暗号化されている場合に、前記鍵データを前記データ提供装置から受ける請求項１９に記載のデータ処理装置。

【請求項２１】処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを用いて構成される請求項１９に記載のデータ処理装置。

【請求項２２】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行うデータ提供システム。

【請求項２３】前記データ提供装置は、前記コンテンツデータを、コンテンツ鍵データを用いて暗号化して前記データ配給装置に提供する請求項２２に記載のデータ提供システム。

【請求項２４】前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを作成し、当該価格データを前記データ処理装置に配給する請求項２２に記載のデータ提供システム。

【請求項２５】前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを、配信鍵データを用いて暗号化して前記データ配給装置に提供し、

前記データ処理装置は、前記配信鍵データを用いて、前記コンテンツ鍵データおよび前記権利書データを復号し、

前記管理装置は、前記配信鍵データを管理し、前記配信鍵データを前記データ提供装置および前記データ処理装置に配給する請求項２３に記載のデータ提供システム。

【請求項２６】前記データ提供装置は、前記暗号化されたコンテンツデータ、前記暗号化されたコンテンツ鍵データおよび前記暗号化された前記権利書データの少なくとも一つのデータに対しての第１の署名データを自らの第１の秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化された鍵データ、前記暗号化された権利書データおよび前記第１の署名データを格納した第１のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第１の秘密鍵データに対応する第１の公開鍵データを用いて前記第１の署名データを検証した後に、自らの第２の秘密鍵データを用いて生成した第２の署名データを前記第１のモジュールに格納

して第２のモジュールを生成し、当該第２のモジュールを前記データ処理装置に配給し、
前記データ処理装置は、前記第１の公開鍵データを用いて、前記配給を受けた前記第２のモジュールに格納された前記第１の署名データを検証し、前記第２の秘密鍵データに対応する第２の公開鍵データを用いて、前記配給を受けた前記第２のモジュールに格納された前記第２の署名データを検証し、
前記管理装置は、前記第１の公開鍵データおよび前記第２の公開鍵データを管理する請求項２５に記載のデータ提供システム。
【請求項２７】前記データ提供装置は、前記第１の公開鍵データを格納した前記第１のモジュールを前記データ配給装置に提供し、
前記データ配給装置は、前記第１の公開鍵データおよび前記第２の公開鍵データを格納した前記第２のモジュールを前記データ処理装置に配給する請求項２６に記載のデータ提供システム。
【請求項２８】前記管理装置は、前記第１の公開鍵データおよび前記第２の公開鍵データを、前記データ処理装置に配給する請求項２６に記載のデータ提供システム。
【請求項２９】前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、
前記管理装置は、前記権利書データ、前記コンテンツデータを前記暗号化する際に用いる鍵データおよび前記価格データのうち少なくとも一つのデータの正当性を認証する請求項２２に記載のデータ提供システム。
【請求項３０】前記データ配給装置は、前記提供された暗号化されたコンテンツデータ、前記提供された権利書データ、前記コンテンツデータを暗号化した前記鍵データおよび前記配給されたコンテンツデータの価格を示す価格データとを格納したモジュールを、前記データ処理装置に配給する請求項２２に記載のデータ提供システム。
【請求項３１】前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記決済処理を行う装置に送信する請求項２２に記載のデータ提供システム。
【請求項３２】前記管理装置は、前記利益分配処理の結果を示す決済レポートデータを、前記データ提供装置および前記データ配給装置の少なくとも一方に送信する請求項３１に記載のデータ提供システム。
【請求項３３】前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記データ提供装置および前記サービス提供装置の少なくとも一方に送信する請求項２２に記載のデータ提供システム。

【請求項３４】前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う請求項２２に記載のデータ提供システム。
【請求項３５】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を制御する請求項２２に記載のデータ提供システム。
【請求項３６】前記データ処理装置の前記第２のモジュールは、その処理内容、予め内部に記憶されたデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである請求項２２に記載のデータ提供システム。
【請求項３７】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う管理装置。
【請求項３８】所定のコンテンツ鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、
前記鍵データを管理する請求項３７に記載の管理装置。
【請求項３９】前記権利書データおよび前記コンテンツ鍵データの少なくとも一方の正当性を認証する請求項３８に記載の管理装置。
【請求項４０】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデータ配給装置から、前記コンテンツデ

ータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記データ配給装置と通信を行う第１のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有するデータ処理装置。

【請求項４１】処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる請求項４０に記載のデータ処理装置。

【請求項４２】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、

前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第１のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第２のモジュールとを有し、

前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行うデータ提供システム。

【請求項４３】コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第１のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第２のモジュールとを有するデータ処理装置。

【請求項４４】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システム。

【請求項４５】前記データ提供装置は、前記コンテンツデータの取り扱いを示す権利書データを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを、前記配給を受けた前記権利書データに基づいて利用し、

前記管理装置は、ルート認証局に対して階層的に下に存在するサブ認証局の役割を果たし、登録された前記データ提供装置、前記データ配給装置および前記データ処理装置で用いられる秘密鍵データに対応する公開鍵データの正当性を証明する際に用いられる公開鍵証明書データの作成および管理と、前記権利書データの認証および前記コンテンツデータに関する権利処理とを行う請求項４４に記載のデータ提供システム。

【請求項４６】前記データ提供装置は、前記鍵データを用いて暗号化して前記データ配給装置に提供し、

前記管理装置は、前記鍵データを管理する請求項４５に記載のデータ提供システム。

【請求項４７】前記データ提供装置および前記データ配給装置の各々は、他の装置との間で認証を行う際に用いられる自らの秘密鍵データを作成し、当該作成した秘密鍵データを管理し、当該秘密鍵データに対応する公開鍵データを作成し、当該公開鍵データと身分証明書および決済口座を前記管理装置に登録し、

前記管理装置は、前記登録に応じて、前記公開鍵データの正当性を証明する公開鍵証明書データを作成する請求

項４５に記載のデータ提供システム。

【請求項４８】前記管理装置は、前記登録に応じて、前記データ提供装置および前記データ配給装置に識別番号をそれぞれ割り振り、前記データ提供装置および前記データ配給装置に、ルート認証局の公開鍵データおよび管理装置の公開鍵データを送信する請求項４７に記載のデータ提供システム。

【請求項４９】前記データ提供装置および前記データ配給装置の各々は、前記秘密鍵データをさらに前記管理装置に登録する請求項４７に記載のデータ提供システム。

【請求項５０】前記データ処理装置には、前記管理装置が生成した秘密鍵データおよび当該秘密鍵データに対応する公開鍵データが予め格納されている請求項４５に記載のデータ提供システム。

【請求項５１】前記データ処理装置には、前記管理装置が生成した前記公開鍵データの正当性を証明する公開鍵証明書データが予め格納されている請求項５０に記載のデータ提供システム。

【請求項５２】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システムにおいて、

前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行うデータ提供システム。

【請求項５３】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他

の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信するデータ提供システム。

【請求項５４】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信するデータ提供システム。

【請求項５５】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを

用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制するデータ提供システム。

【請求項５６】前記管理装置は、不正行為に用いられた前記データ提供装置、前記データ配給装置および前記データ処理装置に対応する公開鍵証明書データを特定する前記公開鍵証明書破棄データを生成する請求項５５に記載のデータ提供システム。

【請求項５７】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項５８】前記管理装置は、前記公開鍵証明書破棄データを前記データ処理装置に直接配給する請求項５７に記載のデータ提供システム。

【請求項５９】前記管理装置は、前記公開鍵証明書破棄データを、前記データ配給装置を介して、放送あるいはオンデマンド方式で前記データ処理装置に配給する請求項５７に記載のデータ提供システム。

【請求項６０】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給を制御するデータ提供システム。

【請求項６１】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御する前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けたコンテンツデータを利用するデータ提供システム。

【請求項６２】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置に

データを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項６３】前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している請求項６２に記載のデータ提供システム。

【請求項６４】前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する請求項６２に記載のデータ提供システム。

【請求項６５】前記データ配給装置は、前記公開鍵証明書破棄データを、放送あるいはオンデマンド方式で前記データ処理装置に配給する請求項６２に記載のデータ提供システム。

【請求項６６】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処

理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項６７】データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御するデータ提供システム。

【請求項６８】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データ

を生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、
前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、
前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、
前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御するデータ提供システム。
【請求項６９】前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している請求項６８に記載のデータ提供システム。
【請求項７０】前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ提供装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する請求項６８に記載のデータ提供システム。
【請求項７１】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、
前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、
前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、
前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御するデータ提供システム。
【請求項７２】前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難

な構成を有している請求項７１に記載のデータ提供システム。
【請求項７３】前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する請求項７１に記載のデータ提供システム。
【請求項７４】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、
前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、
前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、
前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給するデータ提供システム。
【請求項７５】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、
前記データ提供装置は、前記データ配給装置にコンテン

17

ツデータおよび前記公開鍵証明書破棄データを提供し、
前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制するデータ提供システム。

【請求項７６】データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、
前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、
前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制するデータ提供システム。

【請求項７７】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、
前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、
前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、

18

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、
前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有するデータ提供システム。

【請求項７８】前記管理装置は、
前記決済機能を有する第１の管理装置と、
前記権利管理機能を有する第２の管理装置とを有する請求項７７に記載のデータ提供システム。

【請求項７９】前記決済は、電子決済である請求項７７に記載のデータ提供システム。

【請求項８０】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、
前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、
前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、
前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、
前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有するデータ提供システム。

【請求項８１】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有するデータ提供システム。

【請求項８２】データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行うデータ提供方法。

【請求項８３】データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、

前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行うデータ提供方法。

【請求項８４】データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、

前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、

前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行うデータ提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツデータを提供するデータ提供システムおよびその方法と、これらに用いられる管理装置およびデータ処理装置とに関する。

【０００２】

【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このよ

うなデータ提供システムの一つに、音楽データを配信する従来のＥＭＤ(Electronic Music Distribution: 電子音楽配信）システムがある。

【０００３】図６７は、従来のＥＭＤシステム７００の構成図である。図６７に示すＥＭＤシステム７００では、コンテンツプロバイダ７０１ａ，７０１ｂが、サービスプロバイダ７１０に対し、コンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報７０５ａ，７０５ｂ，７０５ｃには、例えば、ＳＣＭＳ(Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ７１０の伝送プロトコルに埋め込んむことを要請する著作権に関する情報などがある。

【０００４】サービスプロバイダ７１０は、受信したコンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとをセッション鍵データを用いて復号する。そして、サービスプロバイダ７１０は、復号したあるいはオフラインで受け取ったコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに、著作権情報７０５ａ，７０５ｂ，７０５ｃを埋め込んで、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを生成する。このとき、サービスプロバイダ７１０は、例えば、著作権情報７０５ａ，７０５ｂ，７０５ｃのうち電子透かし情報をコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにＳＣＭＳ情報を埋め込む。さらに、サービスプロバイダ７１０は、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、鍵データベース７０６から読み出したコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いてそれぞれ暗号化する。その後、サービスプロバイダ７１０は、暗号化されたコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを格納したセキュアコンテナ７２２を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置７０９に存在するＣＡ(Conditional Access)モジュール７１１に送信する。

【０００５】ＣＡモジュール７１１は、セキュアコンテナ７２２をセッション鍵データを用いて復号する。また、ＣＡモジュール７１１は、電子決済やＣＡなどの課金機能を用いて、サービスプロバイダ７１０の鍵データベース７０６からコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置７０９において、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、それぞれコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号することが可能になる。このとき、ＣＡモジュール７１１は、コンテンツ単位で課金処理を行い、その結果に

応じた課金情報７２１を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ７１０の権利処理モジュール７２０に送信する。この場合に、ＣＡモジュール７１１は、サービスプロバイダ７１０が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティー確保とを行う。

【０００６】サービスプロバイダ７１０は、ＣＡモジュール７１１から課金情報７２１を受信すると、サービスプロバイダ７１０とコンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃとの間で利益配分を行う。このとき、サービスプロバイダ７１０から、コンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃへの利益配分は、例えば、ＪＡＳＲＡＣ(Japanese Societyfor Rights of Authors, Composers and Publishers:日本音楽著作権協会）を介して行われる。また、ＪＡＳＲＡＣによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【０００７】また、端末装置７０９では、コンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号したコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、ＲＡＭ型の記録媒体７２３などに記録する際に、著作権情報７０５ａ，７０５ｂ，７０５ｃのＳＣＭＳビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃに埋め込まれたＳＣＭＳビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【０００８】

【発明が解決しようとする課題】ところで、ＳＣＭＳは、ＣＤ(Compact Disc)からＤＡＴ(Digital Audio Tape)への録音を防止するために規定されたものであり、ＤＡＴとＤＡＴとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダなどのコンテンツデータの流通経路を特定するに止まり、違法なコピーを技術的に阻止するものではない。従って、上述した図６７に示すＥＭＤシステム７００では、コンテンツプロバイダの権利（利益）が十分に保護されないという問題がある。

【０００９】また、上述したＥＭＤシステム７００では、ユーザの端末装置７０９からの課金情報７２１を、サービスプロバイダ７１０の権利処理モジュール７２０で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうかが懸念される。

【００１０】また、上述したＥＭＤシステム７００で

は、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

【００１１】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システムおよびその方法、管理装置およびデータ処理装置を提供することを目的とする。また、本発明は、コンテンプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システムおよびその方法、管理装置およびデータ処理装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第１の観点のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

【００１３】本発明の第１の観点のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給する。次に、データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。次に、前記データ処理装置から管理装置に、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを送信する。次に、前記管理装置において、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

【００１４】また、本発明の第２の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【００１５】本発明の第２の観点のデータ提供システムでは、データ提供装置からデータ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供する。次に、前記データ配給装置からデータ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給する。次に、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。次に、前記データ処理装置から前記管理装置に、前記決定した購入形態および利用形態の履歴を示す履歴データを送信する。次に、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【００１６】また、本発明の第３の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示

すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第１のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第２のモジュールとを有し、前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う。

【００１７】また、本発明の第４の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する。

【００１８】また、本発明の第５の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行う。

【００１９】また、本発明の第６の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する。

【００２０】また、本発明の第７の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する。

【００２１】また、本発明の第８の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装

置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する。

【００２２】また、本発明の第９の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する。

【００２３】また、本発明の第１０の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ配給装置は、前記管理装置から前記配給を受けた

公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給を制御する。

【００２４】また、本発明の第１１の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けたコンテンツデータを利用する。

【００２５】また、本発明の第１２の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給

29

した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

【００２６】また、本発明の第１３の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

【００２７】また、本発明の第１４の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果

30

に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

【００２８】また、本発明の第１５の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

【００２９】また、本発明の第１６の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

31

【００３０】また、本発明の第１７の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給する。

【００３１】また、本発明の第１８の観点のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

【００３２】また、本発明の第１９の観点のデータ提供

32

システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

【００３３】また、本発明の第２０の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有する。

【００３４】また、本発明の第２１の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、

33

当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済行う際に用いられる決済請求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する。

【００３５】また、本発明の第２２の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する。

34

【００３６】また、本発明の第１の観点の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う。

【００３７】また、本発明の第２の観点の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【００３８】また、本発明の第１の観点のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信する。

【００３９】また、本発明の第２の観点のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデータ配給装置から、前記コンテンツデータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信する

35

データ処理装置であって、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有する。

【００４０】また、本発明の第３の観点のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第１のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第２のモジュールとを有する。

【００４１】また、本発明の第１の観点のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

【００４２】また、本発明の第２の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入

36

形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

【００４３】また、本発明の第３の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行う。

【００４４】

【発明の実施の形態】以下、本発明の実施形態に係わるＥＭＤ(Electronic Music Distribution: 電子音楽配信）システムについて説明する。

第１実施形態

図１は、本実施形態のＥＭＤシステム１００の構成図である。本実施形態において、ユーザに配信されるコンテンツ(Content）データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。図１に示すように、ＥＭＤシステム１００は、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ（クリアリング・ハウス、以下、ＥＳＣとも記す）１０２およびユーザホームネットワーク１０３を有する。ここで、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２、$SAM105_1$～105_4などが、それぞれ請求項１に係わるデータ提供装置、管理装置およびデータ処理装置に対応している。先ず、ＥＭＤシステム１００の概要について説明する。ＥＭＤシステム１００で

は、コンテンツプロバイダ１０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ１０６を、高い信頼性のある権威機関であるＥＭＤサービスセンタ１０２に送信する。権利書データ１０６は、ＥＭＤサービスセンタ１０２によって権威化（認証）される。

【００４５】また、コンテンツプロバイダ１０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成すると共に、コンテンツ鍵データＫｃをＥＭＤサービスセンタ１０２から配給された対応する期間の配信用鍵データKD_1～KD_{56}で暗号化する。そして、コンテンツプロバイダ１０１は、暗号化されたコンテンツ鍵データＫｃおよびコンテンツファイルＣＦと自らの署名データとを格納したセキュアコンテナ（モジュール）１０４を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク１０３に配給する。

【００４６】ユーザホームネットワーク１０３は、例えば、ネットワーク機器160_1およびＡＶ機器160_2～160_4を有する。ネットワーク機器160_1は、ＳＡＭ(Secure Application Module)105_1を内蔵している。ＡＶ機器160_2～160_4は、それぞれＳＡＭ105_2～105_4を内蔵している。ＳＡＭ105_1～105_4相互間は、例えば、ＩＥＥＥ(Institute ofElectrical and Electronics Engineers)１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

【００４７】ＳＡＭ105_1～105_4は、ネットワーク機器160_1がコンテンツプロバイダ１０１からネットワークなどを介してオンラインで受信したセキュアコンテナ１０４、および／または、コンテンツプロバイダ１０１からＡＶ機器160_2～160_4に記録媒体を介してオフラインで供給されたセキュアコンテナ１０４を対応する期間の配信用鍵データKD_1～KD_3を用いて復号した後に、署名データの検証を行う。ＳＡＭ105_1～105_4に供給されたセキュアコンテナ１０４は、ネットワーク機器160_1およびＡＶ機器160_2～160_4において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。ＳＡＭ105_1～105_4は、上述したセキュアコンテナ１０４の購入・利用の履歴を利用履歴(Usage Log)データ１０８として記録する。利用履歴データ１０８は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じて、ユーザホームネットワーク１０３からＥＭＤサービスセンタ１０２に送信される。

【００４８】ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づいて、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが決済機関９１に支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１に支払われる。また、ＥＭＤサービスセンタ１０２は、一定期間毎に、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【００４９】本実施形態では、ＥＭＤサービスセンタ１０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、ＥＭＤサービスセンタ１０２は、中立の立場にある最高の権威機関であるルート認証局９２に対しての（ルート認証局９２の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ１０１およびＳＡＭ105_1～105_4において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ１０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の権利書データ１０６を登録して権威化することも、ＥＭＤサービスセンタ１０２の認証機能の一つである。また、ＥＭＤサービスセンタ１０２は、例えば、配信用鍵データKD_1～KD_6などの鍵データの管理を行なう鍵データ管理機能を有する。また、ＥＭＤサービスセンタ１０２は、権威化した権利書データ１０６に記述された標準小売価格ＳＲＰ(Suggested Retailer' Price)とＳＡＭ105_1～ＳＡＭ105_4から入力した利用履歴データ１０８とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ１０１に分配する権利処理（利益分配）機能を有する。

【００５０】以下、コンテンツプロバイダ１０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ１０１〕図２は、コンテンツプロバイダ１０１の機能ブロック図であり、ユーザホームネットワーク１０３のＳＡＭ105_1～105_4との間で送受信されるデータに関連するデータの流れが示されている。また、図３には、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間で送受信されるデータに関連するデータの流れが示されている。なお、図３以降の図面では、署名データ処理部、および、セッション鍵データK_{SES}を用いた暗号化・復号部に入出力するデータの流れは省略している。

【００５１】図２および図３に示すように、コンテンツプロバイダ１０１は、コンテンツマスタソースサーバ１１１、電子透かし情報付加部１１２、圧縮部１１３、暗号化部１１４、乱数発生部１１５、暗号化部１１６、署名処理部１１７、セキュアコンテナ作成部１１８、セキュアコンテナデータベース１１８ａ、記憶部１１９、相

互認証部１２０、暗号化・復号部１２１、権利書データ作成部１２２、ＳＡＭ管理部１２４およびＥＭＤサービスセンタ管理部１２５を有する。コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでＥＭＤサービスセンタ１０２に登録し、自らの識別子（識別番号）ＣＰ＿ＩＤを得る。また、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から、ＥＭＤサービスセンタ１０２の公開鍵データと、ルート認証局９２の公開鍵データとを受ける。以下、図２および図３に示すコンテンツプロバイダ１０１の各機能ブロックについて説明する。

【００５２】コンテンツマスタソースサーバ１１１は、ユーザホームネットワーク１０３に提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータＳ１１１を電子透かし情報付加部１１２に出力する。

【００５３】電子透かし情報付加部１１２は、コンテンツデータＳ１１１に対して、ソース電子透かし情報(Source Watermark)Ｗｓ、コピー管理用電子透かし情報(Copy Control Watermark)Ｗｃおよびユーザ電子透かし情報(User Watermark)Ｗｕなどを埋め込んでコンテンツデータＳ１１２を生成し、コンテンツデータＳ１１２を圧縮部１１３に出力する。

【００５４】ソース電子透かし情報Ｗｓは、コンテンツデータの著作権者名、ＩＳＲＣコード、オーサリング日付、オーサリング機器ＩＤ(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Ｗｃは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Ｗｕには、例えば、セキュアコンテナ１０４の配給元および配給先を特定するためのコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよびユーザホームネットワーク１０３のＳＡＭ105_1～105_4の識別子ＳＡＭ＿ID_1～ＳＡＭ＿ID_4が含まれる。また、電子透かし情報付加部１１２は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のＩＤを電子透かし情報としてコンテンツデータＳ１１１に埋め込む。本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、ＥＭＤサービスセンタ１０２において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク１０３内のネットワーク機器160_1およびＡＶ機器160_2～160_4が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク１０３では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容

の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【００５５】圧縮部１１３は、コンテンツデータＳ１１２を、例えば、ＡＴＲＡＣ３(Adaptive Transform Acoustic Coding 3)（商標）などの音声圧縮方式で圧縮し、圧縮したコンテンツデータＳ１１３を暗号化部１１４に出力する。

【００５６】暗号化部１１４は、コンテンツ鍵データＫｃを共通鍵として用い、ＤＥＳ(Data Encryption Standard)やＴｒｉｐｌｅ　ＤＥＳなどの共通鍵暗号化方式で、コンテンツデータＳ１１３を暗号化してコンテンツデータＣを生成し、これをセキュアコンテナ作成部１１８に出力する。また、暗号化部１１４は、コンテンツ鍵データＫｃを共通鍵として用い、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよびメタデータＭｅｔａを暗号化した後に、セキュアコンテナ作成部１１７に出力する。

【００５７】ＤＥＳは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号化方式である。ＤＥＳの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。ＤＥＳの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【００５８】先ず、平文の６４ビットは、上位３２ビットのH_0と下位３２ビットのL_0とに分割される。鍵処理部から供給された４８ビットの拡大鍵データK_1および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を攪拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力との排他的論理和が算出され、その結果はL_1とされる。また、L_0は、H_1とされる。そして、上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【００５９】乱数発生部１１５は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データＫｃとして暗号化部１１４および暗号化部１１６に出力する。なお、コンテンツ鍵データＫｃは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データＫｃは、例えば、所定時間毎に更新される。

【００６０】暗号化部１１６は、後述するようにしてＥＭＤサービスセンタ１０２から受信されて記憶部１１９に記憶された配信用鍵データKD_1～KD_6のうち対応

41

する期間の配信用鍵データKD_1～KD_6を入力し、当該配信用鍵データを共通鍵として用いたＤＥＳなどの共通暗号化方式によって図４（Ｂ）に示すコンテンツ鍵データＫｃ、権利書データ１０６、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3および署名・証明書モジュールMod_1を暗号化した後に、セキュアコンテナ作成部１１７に出力する。署名・証明書モジュールMod_1には、図４（Ｂ）に示すように、署名データ$SIG_{2,CP}$～$SIG_{4,CP}$、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}および当該公開鍵証明書CER_{CP}に対してのＥＭＤサービスセンタ１０２の署名データ$SIG_{1,ESC}$が格納されている。また、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3は、ＳＡＭ105_1～105_4内でプログラムのダウンロードを行なう際に用いられるダウンロード・ドライバと、権利書データ（ＵＣＰ）Ｕ１０６のシンタックス（文法）を示すＵＣＰ－Ｌ(Label)．Ｒ(Reader)と、ＳＡＭ105_1～105_4に内蔵された記憶部（フラッシュＲＯＭ）の書き換えおよび消去をブロック単位でロック状態／非ロック状態にするためのロック鍵データとを格納している。

【００６１】なお、記憶部１１９は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データKD_1～KD_6を記憶するデータベースおよびキーファイルＫＦを記憶するデータベースなどの種々のデータベースを備えている。

【００６２】署名処理部１１７は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いて、その署名データＳＩＧを作成する。

【００６３】なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【００６４】セキュアコンテナ作成部１１８は、図４（Ａ）に示すように、ヘッダデータと、暗号化部１１４から入力したそれぞれコンテンツ鍵データＫｃで暗号化されたコンテンツデータＣ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよびメタデータＭｅｔａとを格納したコンテンツファイルＣＦを生成する。ここで、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔは、ユーザホームネットワーク１０３のネットワーク機器160_1およびＡＶ機器160_2～160_4において、コンテンツファイルＣＦを伸長する際に用いられるソフトウェアであり、例えば、ＡＴＲＡＣ３方式の伸長用ソフトウェアである。

42

【００６５】また、セキュアコンテナ作成部１１８は、図４（Ｂ）に示すように、暗号化部１１６から入力した対応する期間の配信用鍵データKD_1～KD_6で暗号化されたコンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3および署名・証明書モジュールMod_1を格納したキーファイルＫＦを生成する。そして、セキュアコンテナ作成部１１８は、図４（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびキーファイルＫＦと、図４（Ｃ）に示すコンテンツプロバイダ１０１の公開鍵データK_{CP}および署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を生成し、これをセキュアコンテナデータバース１１８ａに格納した後に、ユーザからの要求に応じてＳＡＭ管理部１２４に出力する。このように、本実施形態では、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をセキュアコンテナ１０４に格納してユーザホームネットワーク１０３に送信するイン・バンド(In-band) 方式を採用している。従って、ユーザホームネットワーク１０３は、公開鍵証明書CER_{CP}を得るための通信をＥＭＤサービスセンタ１０２との間で行う必要がない。なお、本発明では、公開鍵証明書CER_{CP}をセキュアコンテナ１０４に格納しないで、ユーザホームネットワーク１０３がＥＭＤサービスセンタ１０２から公開鍵証明書CER_{CP}を得るアウト・オブ・バンド(Out-Of-band) 方式を採用してもよい。

【００６６】相互認証部１２０は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３との間でオンラインでデータを送受信する際に、それぞれＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【００６７】暗号化・復号部１２１は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３にオンラインで送信するデータを、セッション鍵データK_{SES}を用いて暗号化する。また、暗号化・復号部１２１は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３からオンラインで受信したデータを、セッション鍵データK_{SES}を用いて復号する。

【００６８】権利書データ作成部１２２は、権利書データ１０６を作成し、これを暗号化部１１６に出力する。権利書データ１０６は、コンテンツデータＣの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ１０１の運用者が希望する標準小売価格ＳＲＰ(Suggested Retailer' Price) やコンテンツデータＣの複製ルールなどが記述されている。

【００６９】ＳＡＭ管理部１２４は、セキュアコンテナ

１０４を、オフラインおよび／またはオンラインでユーザホームネットワーク１０３に供給する。ＳＡＭ管理部１２４は、ＣＤ－ＲＯＭやＤＶＤなどのＲＯＭ型の記録媒体（メディア）を用いてセキュアコンテナ１０４をオフラインでユーザホームネットワーク１０３に配給する場合には、配信用鍵データKD_1～KD_6などを用いてセキュアコンテナ１０４を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク１０３にオフラインで供給される。

【００７０】図５は、ＲＯＭ型の記録媒体１３０を説明するための図である。図５に示すように、ＲＯＭ型の記録媒体１３０は、ＲＯＭ領域１３１、ＲＡＭ領域１３２およびメディアＳＡＭ１３３を有する。ＲＯＭ領域１３１には、図４（Ａ）に示したコンテンツファイルＣＦが記憶されている。また、ＲＡＭ領域１３２には、図４（Ｂ）、（Ｃ）に示したキーファイルＫＦおよび公開鍵証明書データ$CERT_{CP}$と機器の種類に応じて固有の値を持つ記録用鍵データK_{STR}とを引数としてＭＡＣ関数を用いて生成したと署名データと、当該キーファイルＫＦおよび公開鍵証明書データ$CERT_{CP}$とを記録媒体に固有の値を持つメディア鍵データK_{MED}を用いて暗号化したデータとが記憶される。また、ＲＡＭ領域１３２には、例えば、不正行為などで無効となったコンテンツプロバイダ１０１およびＳＡＭ105_1～105_5を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。また、また、ＲＡＭ領域１３２には、後述するようにユーザホームネットワーク１０３のＳＡＭ105_1～105_4においてコンテンツデータＣの購入・利用形態が決定されたときに生成される利用制御状態（ＵＣＳ）データ１６６などが記憶される。これにより、利用制御状態データ１６６がＲＡＭ領域１３２に記憶されることで、購入・利用形態が決定したＲＯＭ型の記録媒体１３０となる。メディアＳＡＭ１３３には、例えば、ＲＯＭ型の記録媒体１３０の識別子であるメディアＩＤと、メディア鍵データK_{MED}とが記憶されている。メディアＳＡＭ１３３は、例えば、相互認証機能を有している。

【００７１】また、ＳＡＭ管理部１２４は、セキュアコンテナ１０４を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク１０３に配信する場合には、暗号化・復号部１２１においてセッション鍵データK_{SES}を用いてセキュアコンテナ１０４を暗号化した後に、ネットワークを介してユーザホームネットワーク１０３に配信する。本実施形態では、ＳＡＭ管理部、ＥＭＤサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【００７２】ここで、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給は、上述したように記録媒体１３０を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ１０６が格納された共通の形式のセキュアコンテナ１０４を用いる。従って、ユーザホームネットワーク１０３のＳＡＭ105_1～105_4では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ１０６に基づいた権利処理を行なうことができる。

【００７３】また、上述したように、本実施形態では、セキュアコンテナ１０４内に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、当該暗号化を解くためのコンテンツ鍵データＫｃとを同封するイン・バンド(In-Band) 方式を採用している。イン・バンド方式では、ユーザホームネットワーク１０３の機器で、コンテンツデータＣを再生しようとするときに、コンテンツ鍵データＫｃを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データＫｃは配信用鍵データKD_1～KD_6で暗号化されているが、配信用鍵データKD_1～KD_6は、ＥＭＤサービスセンタ１０２で管理されており、ユーザホームネットワーク１０３のＳＡＭ105_1～105_5に事前に（ＳＡＭ105_1～105_4がＥＭＤサービスセンタ１０２に初回にアクセスする際に）配信されているので、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２との間をオンラインで接続することなく、オフラインで、コンテンツデータＣの利用が可能になる。なお、本発明は、コンテンツデータＣとコンテンツ鍵データＫｃとを別々に、ユーザホームネットワーク１０３に供給するアウト・オブ・バンド(Out-Of-Band) 方式を採用できる柔軟性を有している。

【００７４】ＥＭＤサービスセンタ管理部１２５は、ＥＭＤサービスセンタ１０２から６カ月分の配信用鍵データKD_1～KD_6およびそれぞれに対応した署名データ$SIG_{KD1,ESC}$～$SIG_{KD6,ESC}$と、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を含む公開鍵証明書$CERT_{CP}$およびその署名データ$SIG_{1,ESC}$と、決済レポートデータ１０７とを受信すると、これらを暗号化・復号部１２１においてセッション鍵データK_{SES}を用いて復号した後に、記憶部１１９に記憶する。決済レポートデータ１０７は、例えば、ＥＭＤサービスセンタ１０２が図１に示す決済機関９１に対して行なったコンテンツプロバイダ１０１に関する決済の内容が記述されている。

【００７５】また、ＥＭＤサービスセンタ管理部１２５は、提供するコンテンツデータＣのグローバルユニーク(Global Unique) な識別子Ｃｏｎｔｅｎｔ＿ＩＤ、公開鍵データ$K_{CP,P}$およびそれらの署名データ$SIG_{9,CP}$を、ＥＭＤサービスセンタ１０２に送信し、ＥＭＤサービスセンタ１０２から、公開鍵データ$K_{CP,P}$の公開

45

鍵証明書データＣＥＲ$_{CP}$を入力する。また、ＥＭＤサービスセンタ管理部１２５は、権利書データ１０６をＥＭＤサービスセンタ１０２に登録する際に、図６（Ａ）に示すように、提供するコンテンツデータＣのグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤ、コンテンツ鍵データＫｃおよび権利書データ１０６を格納したモジュールＭｏｄ$_3$と、その署名データＳＩＧ$_{5,CP}$とを格納した権利書登録要求用モジュールＭｏｄ$_2$を作成し、これを暗号化・復号部１２１においてセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ネットワークを介してＥＭＤサービスセンタ１０２に送信する。ＥＭＤサービスセンタ管理部１２５としては、前述したように、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【００７６】以下、図２および図３を参照しながら、コンテンツプロバイダ１０１における処理の流れを説明する。なお、以下に示す処理を行う前提として、コンテンツプロバイダ１０１の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ１０２に登録処理を行い、グローバルユニークな識別子ＣＰ＿ＩＤを得ている。識別子ＣＰ＿ＩＤは、記憶部１１９に記憶される。

【００７７】先ず、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２に、自らの秘密鍵データＫ$_{CP,S}$に対応する公開鍵データＫ$_{CP,S}$の正当性を証明する公開鍵証明書データＣＥＲ$_{CP}$を要求する場合の処理を図３を参照しながら説明する。先ず、コンテンツプロバイダ１０１は、真性乱数発生器を用いて乱数を発生して秘密鍵データＫ$_{CP,S}$を生成し、当該秘密鍵データＫ$_{CP,S}$に対応する公開鍵データＫ$_{CP,P}$を作成して記憶部１１９に記憶する。ＥＭＤサービスセンタ管理部１２５は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよび公開鍵データＫ$_{CP,P}$を記憶部１１９から読み出す。そして、ＥＭＤサービスセンタ管理部１２５は、識別子ＣＰ＿ＩＤおよび公開鍵データＫ$_{CP,P}$を、ＥＭＤサービスセンタ１０２に送信する。そして、ＥＭＤサービスセンタ管理部１２５は、当該登録に応じて、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$をＥＭＤサービスセンタ１０２から入力して記憶部１１９に書き込む。

【００７８】次に、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２から配信用鍵データを受信する処理を図３を参照しながら説明する。なお、以下に示す処理を行う前提として、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から既に公開鍵証明書データＣＥＲ$_{CP}$を得ている必要がある。ＥＭＤサービスセンタ管理部１２５が、ＥＭＤサービスセンタ１０２から６カ月分の配信用鍵データＫＤ$_1$～ＫＤ$_3$およびその署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD6,ESC}$を入力し、

46

これを記憶部１１９内の所定のデータベースに記憶する。そして、署名処理部１１７において、記憶部１１９に記憶された署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD6,ESC}$の正当性が確認された後に、記憶部１１９に記憶されている配信用鍵データＫＤ$_1$～ＫＤ$_6$が有効なものとして扱われる。

【００７９】次に、コンテンツプロバイダ１０１がユーザホームネットワーク１０３のＳＡＭ１０５$_1$にセキュアコンテナ１０４を送信する場合の処理を図２を参照しながら説明する。なお、以下の例では、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$にセキュアコンテナ１０４を送信する場合を例示するが、セキュアコンテナ１０４をＳＡＭ１０５$_2$～１０５$_4$に送信する場合も、ＳＡＭ１０５$_1$を介してＳＡＭ１０５$_2$～１０５$_4$に送信される点を除いて同じである。先ず、コンテンツデータＳ１１１がコンテンツマスタソースサーバ１１１から読み出されて電子透かし情報付加部１１２に出力される。次に、電子透かし情報付加部１１２は、コンテンツデータＳ１１１に電子透かし情報を埋め込んでコンテンツデータＳ１１２を生成し、これを圧縮部１１３に出力する。次に、圧縮部１１３は、コンテンツデータＳ１１２を、例えばＡＴＲＡＣ３方式で圧縮してコンテンツデータＳ１１３を作成し、これを暗号化部１１４に出力する。また、乱数発生部１１５から暗号化部１１４に、乱数を発生して生成されたコンテンツ鍵データＫｃが出力される。

【００８０】次に、暗号化部１１４は、コンテンツデータＳ１１３と、記憶部１１９から読み出されたメタデータＭｅｔａおよびＡ／Ｖ伸長用ソフトウェアＳｏｆｔとを、コンテンツ鍵データＫｃを用いて暗号化してセキュアコンテナ作成部１１８に出力する。この場合に、メタデータＭｅｔａは暗号化しなくてもよい。そして、セキュアコンテナ作成部１１８は、図４（Ａ）に示すコンテンツファイルＣＦを作成する。また、署名処理部１１７において、コンテンツファイルＣＦのハッシュ値がとられ、秘密鍵データＫ$_{CP,S}$を用いて署名データＳＩＧ$_{6,CP}$が生成される。

【００８１】また、署名処理部１１７は、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６のそれぞれに対してハッシュ値をとり、秘密鍵データＫ$_{CP,S}$を用いて、それぞれのデータの作成者（提供者）の正当性を示す署名データＳＩＧ$_{2,CP}$，ＳＩＧ$_{3,CP}$，ＳＩＧ$_{4,CP}$を作成する。また、暗号化部１１６は、図４（Ｂ）に示すコンテンツ鍵データＫｃ、権利書データ１０６、ＳＡＭプログラム・ダウンロード・コンテナＳＤ$_1$～ＳＤ$_3$および署名・証明書モジュールＭｏｄ$_1$を、対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$で暗号化してセキュアコンテナ作成部１１８に出力する。そして、セキュアコンテナ作成部１１８は、図４（Ｂ）に示すキーファイルＫＦを作成する。また、署名

47

処理部１１７は、キーファイルＫＦのハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて、署名データ$SIG_{7,CP}$を作成する。

【００８２】次に、セキュアコンテナ作成部１１８は、図４（Ａ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、図４（Ｂ）に示すキーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、図４（Ｃ）に示す公開鍵証明書データＣＥＲ$_{CP}$およびその署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を作成し、これを、セキュアコンテナデータベース１１８ａに記憶する。そして、セキュアコンテナ作成部１１８は、例えばユーザからの要求（リクエスト）に応じてユーザホームネットワーク１０３に提供しようとするセキュアコンテナ１０４をセキュアコンテナデータベース１１８ａから読み出して、相互認証部１２０とＳＡＭ105_1との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部１２１において暗号化した後に、ＳＡＭ管理部１２４を介してユーザホームネットワーク１０３のＳＡＭ105_1に送信する。

【００８３】次に、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２に権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化することを要求する場合の処理を図３を参照して説明する。権利書データ１０６およびコンテンツ鍵データＫｃの権威化要求処理は、個々のコンテンツデータＣ毎に行われる。

【００８４】この場合には、署名処理部１１７において、記憶部１１９から読み出したコンテンツデータＣのグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤ、コンテンツ鍵データＫｃおよび権利書データ作成部１２２から入力した権利書データ１０６からなるモジュールＭｏｄ$_3$のハッシュ値が求められ、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{5,CP}$が生成される。そして、図６（Ａ）に示す権利登録要求用モジュールＭｏｄ$_2$を、相互認証部１２０とＥＭＤサービスセンタ１０２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部１２１において暗号化した後に、ＥＭＤサービスセンタ管理部１２５からＥＭＤサービスセンタ１０２に送信する。

【００８５】本実施形態では、ＥＭＤサービスセンタ１０２において権利書データ１０６およびコンテンツ鍵データＫｃを権威化した後に、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ１０１において配信用鍵データKD_1～KD_6を用いて暗号化を行ってキーファイルＫＦを作成する場合を例示する。但し、本発明は、例えば、ＥＭＤサービスセンタ１０２において権利書データ１０６およびコンテンツ鍵データＫｃを権威化した後に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に、配信用鍵データKD_1～KD_6を用いて暗号化した図６（Ｂ）に示す権威化証明書モジュールＭｏｄ$_{2a}$を送信してもよい。権威化証明書モジュールＭｏｄ$_{2a}$は、コンテンツデータＣのグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤ、コンテンツ鍵データＫｃおよび権利書データ作成部１２２から入力した権利書データ１０６を格納したモジュールＭｏｄ$_{3a}$と、秘密鍵データ$K_{ESC,S}$を用いたモジュールＭｏｄ$_{3a}$の署名データ$SIG_{5a,ESC}$とを格納している。この場合には、コンテンツプロバイダ１０１は、例えば、セキュアコンテナ１０４内に、権威化証明書モジュールＭｏｄ$_{2a}$を格納してＳＡＭ105_1～105_4に配給する。なお、ＥＭＤサービスセンタ１０２は、それぞれ異なる月に対応する配信用鍵データKD_1～KD_6を用いて暗号化した６カ月分の権威化証明書モジュールＭｏｄ$_{2a}$を生成し、これらをまとめてコンテンツプロバイダ１０１に送信してもよい。

48

【００８６】〔ＥＭＤサービスセンタ１０２〕ＥＭＤサービスセンタ１０２は、認証（ＣＡ:Certificate Authority）機能、鍵管理(Key Management)機能および権利処理(Rights Clearing)（利益分配）機能を有する。図７は、ＥＭＤサービスセンタ１０２の機能の構成図である。図７に示すように、ＥＭＤサービスセンタ１０２は、鍵サーバ１４１、鍵データベース１４１ａ、決算処理部１４２、署名処理部１４３、決算機関管理部１４４、証明書・権利書管理部１４５、ＣＥＲデータベース１４５ａ、コンテンツプロバイダ管理部１４８、ＣＰデータベース１４８ａ、ＳＡＭ管理部１４９、ＳＡＭデータベース１４９ａ、相互認証部１５０および暗号化・復号部１５１を有する。なお、図７には、ＥＭＤサービスセンタ１０２内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ１０１との間で送受信されるデータに関連するデータの流れが示されている。また、図８には、ＥＭＤサービスセンタ１０２内の機能ブロック相互間のデータの流れのうち、ＳＡＭ105_1～105_4および図１に示す決済機関９１との間で送受信されるデータに関連するデータの流れが示されている。

【００８７】鍵サーバ１４１は、鍵データベース１４１ａに記憶された各々有効期間が１カ月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部１４８およびＳＡＭ管理部１４９に出力する。また、鍵データベース１４１ａ配信用鍵データＫＤの他に、記録用鍵データK_{STR}、メディア鍵データK_{MED}およびＭＡＣ鍵データK_{MAC}などの鍵データを記憶する一連の鍵データースからなる。

【００８８】決算処理部１４２は、ＳＡＭ105_1～105_4から入力した利用履歴データ１０８と、証明書・権利書管理部１４５から入力した標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済レポートデータ１０７および決済請求権データ１５２を作成し、決済レポートデータ１０７をコンテンツプロバ

イダ管理部１４８に出力し、決済請求権データ１５２を決算機関管理部１４４に出力する。なお、決算処理部１４２は、販完価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。ここで、利用履歴データ１０８は、ユーザホームネットワーク１０３におけるセキュアコンテナ１０４の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部１４２においてセキュアコンテナ１０４に関連したラインセンス料の支払い額を決定する際に用いられる。

【００８９】利用履歴データ１０８には、例えば、セキュアコンテナ１０４に格納されたコンテンツデータＣの識別子Ｃｏｎｔｅｎｔ＿ＩＤ、セキュアコンテナ１０４を配給したコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、セキュアコンテナ１０４内のコンテンツデータＣの圧縮方法、セキュアコンテナ１０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ１０４を配給を受けたＳＡＭ105_1～105_4の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭ105_1～105_4のユーザのＵＳＥＲ＿ＩＤなどが記述されている。従って、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク１０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ１０７および決済請求権データ１５２を作成する。当該分配率表は、例えば、セキュアコンテナ１０４に格納されたコンテンツデータ毎に作成される。また、決済請求権データ１５２は、当該データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。なお、決済機関９１は、決済が終了すると、当該決済機関の利用明細書をＥＭＤサービスセンタ１０２に送る。ＥＭＤサービスセンタ１０２は、当該利用明細書の内容を、対応する権利者に通知する。

【００９０】決算機関管理部１４４は、決算処理部１４２が生成した決済請求権利データ１５２を図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。なお、後述するように、決算機関管理部１４４は、決済請求権データ１５２を、コンテンツプロバイダ１０１などの権利者に送信し、権利者自らが、受信した決済請求権データ１５２を用いて決済機関９１に決済を行ってもよい。また、決算機関管理部１４４は、署名処理部１４３において決済請求権データ１５２のハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いて生成した署名データＳＩＧ$_{99}$を決済請求権データ１５２と共に決済機関９１に送信する。

【００９１】証明書・権利書管理部１４５は、ＣＥＲデータベース１４５ａに登録されて権威化された公開鍵証

明書データＣＥＲ$_{CP}$および公開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$などを読み出すと共に、コンテンツプロバイダ１０１の権利書データ１０６およびコンテンツ鍵データＫｃなどをＣＥＲデータベース１４５ａに登録して権威化する。なお、公開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$を格納するデータースと、権利書データ１０６およびコンテンツ鍵データＫｃとを個別に設けてもよい。このとき、証明書・権利書管理部１４５は、例えば、権利書データ１０６およびコンテンツ鍵データＫｃなどのハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いた署名データを付した権威化されたそれぞれの証明書データを作成する。

【００９２】コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１との間で通信する機能を有し、登録されたコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤなどを管理するＣＰデータベース１４８ａにアクセスできる。

【００９３】ＳＡＭ管理部１４９は、ユーザホームネットワーク１０３内のＳＡＭ105_1～105_4との間で通信する機能を有し、登録されたＳＡＭの識別子ＳＡＭ＿ＩＤやＳＡＭ登録リストなどを記録したＳＡＭデータベース１４９ａにアクセスできる。

【００９４】以下、ＥＭＤサービスセンタ１０２内での処理の流れを説明する。先ず、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１およびユーザホームネットワーク１０３内のＳＡＭ105_1～105_4への配信用鍵データを送信する際の処理の流れを、図７および図８を参照しながら説明する。図７に示すように、鍵サーバ１４１は、所定期間毎に、例えば、６カ月分の配信用鍵データKD_1～KD_6を鍵データベース１４１ａから読み出してコンテンツプロバイダ管理部１４８に出力する。また、署名処理部１４３は、配信用鍵データKD_1～KD_6の各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、それぞれに対応する署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD6,ESC}$を作成し、これをコンテンツプロバイダ管理部１４８に出力する。コンテンツプロバイダ管理部１４８は、この６カ月分の配信用鍵データKD_1～KD_6およびそれらの署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD6,ESC}$を、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【００９５】また、図８に示すように、鍵サーバ１４１は、所定期間毎に、例えば、３カ月分の配信用鍵データKD_1～KD_3を鍵データベース１４１ａから読み出してＳＡＭ管理部１４９に出力する。また、署名処理部１４３は、配信用鍵データKD_1～KD_3の各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、それぞれに対応する署名データＳ

ＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$を作成し、これをＳＡＭ管理部１４９に出力する。ＳＡＭ管理部１４９は、この３カ月分の配信用鍵データＫＤ$_1$～ＫＤ$_3$およびそれらの署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$を、相互認証部１５０とＳＡＭ１０５$_1$～１０５$_4$と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ＳＡＭ１０５$_1$～１０５$_4$に送信する。

【００９６】次に、ＥＭＤサービスセンタ１０２がコンテンツプロバイダ１０１から、公開鍵証明書データＣＥＲ$_{CP}$の発行要求を受けた場合の処理を、図７を参照しながら説明する。この場合に、コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、公開鍵データＫ$_{CP,P}$および署名データＳＩＧ$_{9,CP}$をコンテンツプロバイダ１０１から受信すると、これらを、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて復号する。そして、当該復号した署名データＳＩＧ$_{9,CP}$の正当性を署名処理部１４３において確認した後に、識別子ＣＰ＿ＩＤおよび公開鍵データＫ$_{CP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ１０１がＣＰデータベース１４８ａに登録されているか否かを確認する。そして、証明書・権利書管理部１４５は、当該コンテンツプロバイダ１０１の公開鍵証明書データＣＥＲ$_{CP}$をＣＥＲデータベース１４５ａから読み出してコンテンツプロバイダ管理部１４８に出力する。また、署名処理部１４３は、公開鍵証明書データＣＥＲ$_{CP}$のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データＫ$_{ESC,S}$を用いて、署名データＳＩＧ$_{1,ESC}$を作成し、これをコンテンツプロバイダ管理部１４８に出力する。そして、コンテンツプロバイダ管理部１４８は、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$を、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【００９７】次に、ＥＭＤサービスセンタ１０２がＳＡＭ１０５$_1$から、公開鍵証明書データＣＥＲ$_{SAM1}$の発行要求を受けた場合の処理を、図８を参照しながら説明する。この場合に、ＳＡＭ管理部１４９は、ＳＡＭ１０５$_1$の識別子ＳＡＭ$_1$＿ＩＤ、公開鍵データＫ$_{SAM1,P}$および署名データＳＩＧ$_{8,SAM1}$をＳＡＭ１０５$_1$から受信すると、これらを、相互認証部１５０とＳＡＭ１０５$_1$と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて復号する。そして、当該復号した署名データＳＩＧ$_{8,SAM1}$の正当性を署名処理部１４３において確認した後に、識別子ＳＡＭ$_1$＿ＩＤおよび公開鍵データＫ$_{SAM1,P}$に基づいて、当該公開鍵証明書データの発行要求を出したＳＡＭ１０５$_1$がＳＡＭデータベース１４９ａに登録されているか否かを確認する。そして、証明書・権利書管理部１４５は、当該ＳＡＭ１０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$をＣＥＲデータベース１４５ａから読み出してＳＡＭ管理部１４９に出力する。

た、署名処理部１４３は、公開鍵証明書データＣＥＲ$_{SAM1}$のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データＫ$_{ESC,S}$を用いて、署名データＳＩＧ$_{50,ESC}$を作成し、これをＳＡＭ管理部１４９に出力する。そして、ＳＡＭ管理部１４９は、公開鍵証明書データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{50,ESC}$を、相互認証部１５０とＳＡＭ１０５$_1$と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ＳＡＭ１０５$_1$に送信する。なお、ＳＡＭ１０５$_2$～１０５$_4$が、公開鍵証明書データを要求した場合の処理は、対象がＳＡＭ１０５$_2$～１０５$_4$に代わるのみで、基本的に上述したＳＡＭ１０５$_1$の場合と同じである。なお、本発明では、ＥＭＤサービスセンタ１０２は、例えば、ＳＡＭ１０５$_1$の出荷時に、ＳＡＭ１０５$_1$の秘密鍵データＫ$_{SAM1,S}$および公開鍵データＫ$_{SAM1,P}$をＳＡＭ１０５$_1$の記憶部に記憶する場合には、当該出荷時に、公開鍵データＫ$_{SAM1,P}$の公開鍵証明書データＣＥＲ$_{SAM1}$を作成してもよい。このとき、当該出荷時に、公開鍵証明書データＣＥＲ$_{SAM1}$を、ＳＡＭ１０５$_1$の記憶部に記憶してもよい。

【００９８】次に、ＥＭＤサービスセンタ１０２が、コンテンツプロバイダ１０１から権利書データ１０６およびコンテンツ鍵データＫｃの登録要求を受けた場合の処理を、図７を参照しながら説明する。この場合には、コンテンツプロバイダ管理部１４８がコンテンツプロバイダ１０１から図６（Ａ）に示す権利書登録要求モジュールＭｏｄ$_2$を受信すると、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて権利書登録要求モジュールＭｏｄ$_2$を復号する。そして、署名処理部１４３において、鍵データベース１４１ａから読み出した公開鍵データＫ$_{cp}$を用いて、署名データＳＩＧ$_{5,CP}$の正当性を検証する。次に、証明書・権利書管理部１４５は、権利書登録要求モジュールＭｏｄ$_2$に格納された権利書データ１０６およびコンテンツ鍵データＫｃを、ＣＥＲデータベース１４５ａに登録する。

【００９９】次に、ＥＭＤサービスセンタ１０２において決済処理を行なう場合の処理を図８を参照しながら説明する。ＳＡＭ管理部１４９は、ユーザホームネットワーク１０３の例えばＳＡＭ１０５$_1$から利用履歴データ１０８およびその署名データＳＩＧ$_{200,SAM1}$を入力すると、利用履歴データ１０８および署名データＳＩＧ$_{200,SAM1}$を、相互認証部１５０とＳＡＭ１０５$_1$との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて復号し、ＳＡＭ１０５$_1$の公開鍵データＫ$_{SAM1}$による署名データＳＩＧ$_{200,SAM1}$の検証を行なった後に、決算処理部１４２に出力する。

【０１００】そして、決算処理部１４２は、ＳＡＭ管理部１４９から入力した利用履歴データ１０８と、証明書

53

・権利書管理部１４５を介してＣＥＲデータベース１４５ａから読み出した権利書データ１０６に含まれる標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を生成する。決算処理部１４２は、決済請求権データ１５２を決算機関管理部１４４に出力すると共に、決済レポートデータ１０７をコンテンツプロバイダ管理部１４８に出力する。

【０１０１】次に、決算機関管理部１４４は、決済請求権データ１５２およびその署名データＳＩＧ$_{99}$を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。これにより、決済請求権データ１５２に示される金額の金銭が、コンテンツプロバイダ１０１に支払われる。

【０１０２】次に、ＥＭＤサービスセンタ１０２がコンテンツプロバイダ１０１に決済レポートを送信する場合の処理を図７を参照しながら説明する。決算処理部１４２において決済が行なわれると、前述したように、決算処理部１４２からコンテンツプロバイダ管理部１４８に決済レポートデータ１０７が出力される。決済レポートデータ１０７は、上述したように、例えば、ＥＭＤサービスセンタ１０２が図１に示す決済機関９１に対して行なったコンテンツプロバイダ１０１に関する決済の内容が記述されている。ＥＭＤサービスセンタ１０２は、決算処理部１４２から決済レポートデータ１０７を入力すると、これを、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１０３】また、ＥＭＤサービスセンタ１０２は、前述したように、権利書データ１０６を登録（権威化）した後に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に、図６（Ｂ）に示す権威化証明書モジュールMod_{2a}を配信用鍵データKD_1～KD_6で暗号化して送信してもよい。

【０１０４】また、ＥＭＤサービスセンタ１０２は、その他に、ＳＡＭ105_1～105_4の出荷時の処理と、ＳＡＭ登録リストの登録処理とを行なうが、これらの処理については後述する。

【０１０５】〔ユーザホームネットワーク１０３〕ユーザホームネットワーク１０３は、図１に示すように、ネットワーク機器160_1およびＡ／Ｖ機器160_2～160_4を有している。ネットワーク機器160_1は、ＳＡＭ105_1を内蔵している。また、ＡＶ機器160_2～160_4は、それぞれＳＡＭ105_2～105_4を内蔵している。ＳＡＭ105_1～105_4の相互間は、例えば、ＩＥＥＥ１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。なお、ＡＶ機器160_2～160_4は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器160_1のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク１０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

54

【０１０６】以下、ネットワーク機器160_1について説明する。図９は、ネットワーク機器160_1の構成図である。図９に示すように、ネットワーク機器160_1は、ＳＡＭ105_1、通信モジュール１６２、復号・伸長モジュール１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。

【０１０７】ＳＡＭ105_1～105_4は、コンテンツ単位の課金処理をおこなうモジュールであり、ＥＭＤサービスセンタ１０２との間で通信を行う。ＳＡＭ105_1～105_4は、例えば、ＥＭＤサービスセンタ１０２によって仕様およびバージョンなどが管理され、家庭機器メーカに対し、搭載の希望があればコンテンツ単位の課金を行うブラックスボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、ＳＡＭ105_1～105_4のＩＣ(Integrated Circuit)の内部の仕様を知ることはできず、ＥＭＤサービスセンタ１０２が当該ＩＣのインタフェースなどを統一化し、それに従ってネットワーク機器160_1およびＡＶ機器160_2～160_4に搭載される。

【０１０８】ＳＡＭ105_1～105_4は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Registance) 性を持ったハードウェアモジュール（ＩＣモジュールなど）である。ＳＡＭ105_1～105_4の機能をＩＣという形で実現する場合は、ＩＣ内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。ＳＡＭをＩＣという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をＳＡＭとして定義してもよい。

【０１０９】以下、ＳＡＭ105_1の機能について詳細に説明する。なお、ＳＡＭ105_2～105_4は、ＳＡＭ105_1と基本的に同じ機能を有している。図１０は、ＳＡＭ105_1の機能の構成図である。なお、図１０には、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力し、セキュアコンテナ１０４内のキーファイルＫＦを復号する処理に関連するデータの流れが示されている。図１０に示すように、ＳＡＭ105_1は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、コンテンツプロバイダ管理部１８０、誤り訂正部１８１、ダウンロードメモリ管理部１８２、セキュアコンテナ復号部１８３、復号・伸長モジュール管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監

視部１８６、課金処理部１８７、署名処理部１８９、ＳＡＭ管理部１９０、メディアＳＡＭ管理部１９７、スタック（作業）メモリ２００および外部メモリ管理部８１１を有する。なお、ＡＶ機器160_2～160_4はダウンロードメモリ１６７を有していないため、ＳＡＭ105_2～105_4にはダウンロードメモリ管理部１８２は存在しない。

【０１１０】なお、図１０に示すＳＡＭ105_1の所定の機能は、例えば、図示しないＣＰＵにおいて秘密プログラムを実行することによって実現される。また、スタックメモリ２００には、以下に示す処理を経て、図１１に示すように、利用履歴データ１０８およびＳＡＭ登録リストが記憶される。ここで、外部メモリ２０１のメモリ空間は、ＳＡＭ105_1の外部（例えば、ホストＣＰＵ８１０）からは見ることはできず、ＳＡＭ105_1のみが外部メモリ２０１の記憶領域に対してのアクセスを管理できる。外部メモリ２０１としては、例えば、フラッシュメモリあるいは強誘電体メモリ（ＦｅＲＡＭ）などが用いられる。また、スタックメモリ２００としては、例えばＳＡＲＡＭが用いられ、図１２に示すように、セキュアコンテナ１０４、コンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOC}、コンテンツプロバイダ１０１の公開鍵証明書CER_{CP}、利用制御状態データ（ＵＣＳ）１６６、およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3などが記憶される。

【０１１１】以下、ＳＡＭ105_1の機能のうち、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力したときの各機能ブロックの処理内容を図１０を参照しながら説明する。

【０１１２】相互認証部１７０は、ＳＡＭ105_1がコンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間でオンラインでデータを送受信する際に、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成し、これを暗号化・復号部１７１に出力する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【０１１３】暗号化・復号部１７１は、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で送受信するデータを、相互認証部１７０が生成したセッション鍵データK_{SES}を用いて暗号化・復号する。

【０１１４】誤り訂正部１８１は、セキュアコンテナ１０４を誤り訂正してダウンロードメモリ管理部１８２に出力する。なお、ユーザホームネットワーク１０３は、セキュアコンテナ１０４が改竄されているか否かを検出する機能を有していてもよい。本実施形態では、誤り訂正部１８１を、ＳＡＭ105_1に内蔵した場合を例示したが、誤り訂正部１８１の機能を、例えばホストＣＰＵ８１０などのＳＡＭ105_1の外部に持たせてもよい。

【０１１５】ダウンロードメモリ管理部１８２は、図９に示すようにダウンロードメモリ１６７が相互認証機能を持つメディアＳＡＭ１６７ａを有している場合には、相互認証部１７０とメディアＳＡＭ１６７ａとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ１０４を、相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化して図９に示すダウンロードメモリ１６７に書き込む。ダウンロードメモリ１６７としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図１３に示すように、ＨＤＤ（Hard Disk Drive）などの相互認証機能を備えていないメモリをダウンロードメモリ２１１として用いる場合には、ダウンロードメモリ２１１内はセキュアではないので、コンテンツファイルＣＦをダウンロードメモリ２１１にダウンロードし、機密性の高いキーファイルＫＦを例えば、図１０に示すスタックメモリ２００にダウンロードする。

【０１１６】セキュアコンテナ復号部１８３は、ダウンロードメモリ管理部１８２から入力したセキュアコンテナ１０４に格納されたキーファイルＫＦを、記憶部１９２から読み出した対応する期間の配信用鍵データKD_1～KD_3を用いて復号し、署名処理部１８９において署名データ$SIG_{2,CP}$～$SIG_{4,CP}$の正当性、すなわちコンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の作成者の正当性を確認した後に、スタックメモリ２００に書き込む。

【０１１７】ＥＭＤサービスセンタ管理部１８５は、図１に示すＥＭＤサービスセンタ１０２との間の通信を管理する。

【０１１８】署名処理部１８９は、記憶部１９２から読み出したＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$およびコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、セキュアコンテナ１０４内の署名データの検証を行なう。

【０１１９】記憶部１９２は、ＳＡＭ105_1の外部から読み出しおよび書き換えできない秘密データとして、図１４に示すように、配信用鍵データKD_1～KD_3、ＳＡＭ＿ＩＤ、ユーザＩＤ、パスワード、情報参照用ＩＤ、ＳＡＭ登録リスト、記録用鍵データK_{STR}、ルートＣＡの公開鍵データ$K_{R\text{-}CA,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、メディア鍵データK_{MED}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ105_1の秘密鍵データ$K_{SAM1,S}$、ＳＡＭ105_1の公開鍵データ$K_{SAM1,P}$を格納した公開鍵証明書CER_{SAM1}、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いた公開鍵証明書CER_{ESC}の署名データSIG_{22}、復号・伸長モジュール１６３との間の相互認証用の元鍵データ、メディアＳＡＭとの間の相互認証用の元鍵データを記憶している。また、記憶部１９２には、図１０に示す少なくとも一部の機能を実現する

ための秘密プログラムが記憶されている。記憶部１９２としては、例えば、フラッシューＥＥＰＲＯＭ(Electrically Erasable Programmable RAM)が用いられる。

【０１２０】以下、ＥＭＤサービスセンタ１０２から受信した配信用鍵データKD_1～KD_3を記憶部１９２に格納する際のＳＡＭ105_1内での処理の流れを図１０を参照しながら説明する。この場合には、先ず、相互認証部１７０と図７に示す相互認証部１５０との間で相互認証が行われる。次に、当該相互認証によって得られたセッション鍵データK_{SES}で暗号化された３カ月分の配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$が、ＥＭＤサービスセンタ１０２からＥＭＤサービスセンタ管理部１８５を介してスタックメモリ８１１に書き込まれる。次に、暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて、配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$が復号される。次に、署名処理部１８９において、スタックメモリ８１１にに記憶された署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$の正当性が確認された後に、配信用鍵データKD_1～KD_3が記憶部１９２に書き込まれる。

【０１２１】以下、セキュアコンテナ１０４をコンテンツプロバイダ１０１から入力し、セキュアコンテナ１０４内のキーファイルＫＦを復号する際のＳＡＭ105_1内での処理の流れを図１０を参照しながら説明する。図１０に示すＳＡＭ105_1の相互認証部１７０と図２に示す相互認証部１２０との間で相互認証が行なわれる。暗号化・復号部１７１は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、コンテンツプロバイダ管理部１８０を介してコンテンツプロバイダ１０１から供給されたセキュアコンテナ１０４を復号する。

【０１２２】次に、署名処理部１８９は、図４（Ｃ）に示す署名データ$SIG_{1,ESC}$の検証を行なった後に、図４（Ｃ）に示す公開鍵証明書データCER_{CP}内に格納されたコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の正当性を確認する。コンテンツプロバイダ管理部１８０は、署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の正当性が確認されると、セキュアコンテナ１０４を誤り訂正部１８１に出力する。

【０１２３】誤り訂正部１８１は、セキュアコンテナ１０４を誤り訂正した後に、ダウンロードメモリ管理部１８２に出力する。ダウンロードメモリ管理部１８２は、相互認証部１７０と図９に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ１０４をダウンロードメモリ１６７に書き込む。

【０１２４】次に、ダウンロードメモリ管理部１８２は、相互認証部１７０と図９に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ１０４に格納された図４（Ｂ）に示すキーファイルＫＦをダウンロードメモリ１６７から読み出してセキュアコンテナ復号部１８３に出力する。

【０１２５】そして、セキュアコンテナ復号部１８３は、記憶部１９２から入力した対応する期間の配信用鍵データKD_1～KD_3を用いて、キーファイルＫＦを復号し、図４（Ｂ）に示す署名・証明書モジュールＭｏｄ１に格納された署名データ$SIG_{1,ESC}$、$SIG_{2,CP}$～$SIG_{4,CP}$を署名処理部１８９に出力する。署名処理部１８９は、図４（Ｂ）に示す署名データ$SIG_{1,ESC}$の検証を行なった後に、図４（Ｂ）に示す公開鍵証明書データCER_{CP}内に格納された公開鍵データ$K_{ESC,P}$を用いて署名データ$SIG_{2,CP}$～$SIG_{4,CP}$の検証を行なう。これにより、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の作成者の正当性が検証される。

【０１２６】次に、セキュアコンテナ復号部１８３は、署名データ$SIG_{2,CP}$～$SIG_{4,CP}$の正当性が確認されると、キーファイルＫＦをスタックメモリ２００に書き込む。

【０１２７】以下、ダウンロードメモリ１６７にダウンロードされたコンテンツデータＣを利用・購入する処理に関連する各機能ブロックの処理内容を図１５を参照しながら説明する。

【０１２８】利用監視部１８６は、スタックメモリ２００から権利書データ１０６および利用制御状態データ１６６を読み出し、当該読み出した権利書データ１０６および利用制御状態データ１６６によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ１０６は、図１０を用いて説明したように、復号後にスタックメモリ２００に記憶された図４（Ｂ）に示すキーファイルＫＦ内に格納されている。また、利用制御状態データ１６６は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ２００に記憶される。

【０１２９】課金処理部１８７は、図９に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５に応じた利用履歴データ１０８を作成する。ここで、利用履歴データ１０８は、前述したように、ユーザによるセキュアコンテナ１０４の購入および利用の形態の履歴を記述しており、ＥＭＤサービスセンタ１０２において、セキュアコンテナ１０４の購入に応じた決済処理およびラインセンス料の支払いを決定する際に用いられる。

【０１３０】また、課金処理部１８７は、必要に応じて、スタックメモリ２００から読み出した販売価格あるいは標準小売価格データＳＲＰをユーザに通知する。ここで、販売価格および標準小売価格データＳＲＰは、復号後にスタックメモリ２００に記憶された図４（Ｂ）に示すキーファイルＫＦの権利書データ１０６内に格納されている。課金処理部１８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用

許諾条件などの権利内容および利用制御状態データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【０１３１】また、課金処理部１８７は、操作信号Ｓ１６５に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態（UCS: Usage Control Status）データ１６６を生成し、これをスタックメモリ２００書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ１６６には、コンテンツのＩＤ、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０１３２】なお、決定された購入形態が再生課金である場合には、例えば、$SAM105_1$からコンテンツプロバイダ１０１に利用制御状態データ１６６をコンテンツデータＣの購入と同時にリアルタイムに送信し、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２に、利用履歴データ１０８を所定の期間内に$SAM105_1$に取りにいくことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ１６６が、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ１６６をコンテンツプロバイダ１０１にリアルタイムに送信する。

【０１３３】ＥＭＤサービスセンタ管理部１８５は、外部メモリ管理部８１１を介して外部メモリ２０１から読み出した利用履歴データ１０８をＥＭＤサービスセンタ１０２に送信する。このとき、ＥＭＤサービスセンタ管理部１８５は、署名処理部１８９において、秘密鍵データ$K_{SAM1,S}$を用いて利用履歴データ１０８の署名データ$SIG_{200,SAM1}$を作成し、署名データ$SIG_{200,SAM1}$を利用履歴データ１０８と共にＥＭＤサービスセンタ１０２に送信する。ＥＭＤサービスセンタ１０２への利用履歴データ１０８の送信は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ１０８に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ２０１の記憶容量に応じて決定される。

【０１３４】ダウンロードメモリ管理部１８２は、例えば、図９に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツデータＣ、スタックメモリ２００から読み出したコンテンツ鍵データK_cおよび課金処理部１８７から入力したユーザ電子透かし情報用データ１９６を復号・伸長モジュール管理部１８４に出力する。また、復号・伸長モジュール管理部１８４は、図９に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツファイルＣＦ、並びにスタックメモリ２００から読み出したコンテンツ鍵データK_cおよび半開示パラメータデータ１９９を復号・伸長モジュール管理部１８４に出力する。

【０１３５】ここで、半開示パラメータデータ１９９は、権利書データ１０６内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール１６３では、半開示パラメータデータ１９９に基づいて、暗号化されたコンテンツデータＣを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール１６３がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ１９９によって、コンテンツ鍵データK_cを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【０１３６】以下、$SAM105_1$内での処理の流れについて説明する。先ず、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでの処理の流れを図１５を参照しながら説明する。先ず、ユーザによる図９に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が課金処理部１８７に出力されると、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、復号・伸長モジュール管理部１８４を介して、図９に示す復号・伸長モジュール１６３に出力される。このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。コンテンツファイルＣＦは、図９に示す復号部２２１において復号された後に、復号部２２２に出力される。

【０１３７】また、スタックメモリ２００から読み出されたコンテンツ鍵データK_cおよび半開示パラメータデータ１９９が、図９に示す復号・伸長モジュール１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫ

61

ｃおよび半開示パラメータデータ１９９に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。次に、電子透かし情報処理部２２４においてユーザ電子透かし情報用データ１９６がコンテンツデータＣに埋め込まれた後、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。

【０１３８】そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。そして、課金処理部１８７において、決定された購入形態に応じた利用履歴データ１０８および利用制御状態データ１６６が生成され、利用履歴データ１０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に、利用制御状態データ１６６がスタックメモリ２００に書き込まれる。以後は、利用監視部１８６において、利用制御状態データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。そして、スタックメモリ２００に格納されているキーファイルＫＦに、利用制御状態データ１６６が加えられ、購入形態が決定した後述する図１８（Ｂ）に示す新たなキーファイルKF_1が生成される。キーファイルKF_1は、スタックメモリ２００に記憶される。図１８（Ｂ）に示すように、キーファイルKF_1に格納された利用制御状態データ１６６はストレージ鍵データK_{STR}を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をＭＡＣ(Message Authentication Code) 鍵データとして用いて生成したＭＡＣ値であるMAC_{300}が付されている。また、利用制御状態データ１６６およびMAC_{300}からなるモジュールは、メディア鍵データK_{MED}を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データK_{MED}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{301}が付されている。

【０１３９】次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図１５を参照しながら説明する。この場合には、利用監視部１８６の監視下で、操作信号Ｓ１６５に基づいて、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、図９に示す復号・伸長モジュール１６３に出力される。このとき、図１５に示す相互認証部１７０と、図９に示す

62

復号・伸長モジュール１６３の相互認証部２２０との間で相互認証が行われる。また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃが復号・伸長モジュール１６３に出力される。そして、復号・伸長モジュール１６３の復号部２２２において、コンテンツ鍵データＫｃを用いたコンテンツファイルＣＦの復号と、伸長部２２３による伸長処理とが行なわれ、再生モジュール１６９において、コンテンツデータＣが再生される。このとき、課金処理部１８７によって、操作信号Ｓ１６５に応じて、外部メモリ２０１に記憶されている利用履歴データ１０８が更新される。利用履歴データ１０８は、外部メモリ２０１から読み出された後、相互認証を経て、ＥＭＤサービスセンタ管理部１８５を介して、署名データ$SIG_{200,SAM1}$と共にＥＭＤサービスセンタ１０２に送信される。

【０１４０】次に、図１６に示すように、例えば、ネットワーク機器160_1のダウンロードメモリ１６７にダウンロードされた既に購入形態が決定されたコンテンツファイルＣＦおよびキーファイルＫＦを、バス１９１を介して、ＡＶ機器160_2のＳＡＭ105_2に転送する場合のＳＡＭ105_1内での処理の流れを図１７を参照しながら説明する。ユーザは、購入・利用形態決定操作部１６５を操作して、ダウンロードメモリ１６７に記憶された所定のコンテンツをＡＶ機器160_2に転送することを指示し、当該操作に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。これにより、課金処理部１８７は、操作信号Ｓ１６５に基づいて、外部メモリ２０１に記憶されている利用履歴データ１０８を更新する。

【０１４１】また、ダウンロードメモリ管理部１８２は、ダウンロードメモリ１６７から読み出した図１８（Ａ）に示すコンテンツファイルＣＦをＳＡＭ管理部１９０に出力する。また、スタックメモリ２００から読み出した図１８（Ｂ）に示すキーファイルKF_1を、署名処理部１８９およびＳＡＭ管理部１９０に出力する。署名処理部１８９は、スタックメモリ２００から読み出したキーファイルKF_1の署名データ$SIG_{42,SAM1}$を作成し、これをＳＡＭ管理部１９０に出力する。また、ＳＡＭ管理部１９０は、記憶部１９２から、図１８（Ｃ）に示す公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$を読み出す。

【０１４２】また、相互認証部１７０は、ＳＡＭ105_2との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部１７１に出力する。ＳＡＭ管理部１９０は、図１８（Ａ），（Ｂ），（Ｃ）に示すデータからなる新たなセキュアコンテナを購入、暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて暗号化した後に、図１６に示すＡＶ機器160_2のＳＡＭ105_2に出力する。このとき、ＳＡＭ105_1とＳＡＭ105_2との間の相互認証と並行して、ＩＥＥＥ１

３９４シリアルバスであるバス１９１の相互認証が行われる。

【０１４３】以下、図１６に示すように、ＳＡＭ１０５$_1$から入力したコンテンツファイルＣＦなどを、ＲＡＭ型などの記録媒体（メディア）に書き込む際のＳＡＭ１０５$_2$内での処理の流れを、図１９を参照しながら説明する。

【０１４４】この場合には、ＳＡＭ１０５$_2$のＳＡＭ管理部１９０は、図１６に示すように、図１８（Ａ）に示すコンテンツファイルＣＦと、図１８（Ｂ）に示すキーファイルKF_1およびその署名データ$SIG_{42,SAM1}$と、図１８（Ｃ）に示す公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とを、ネットワーク機器１６０$_1$のＳＡＭ１０５$_1$から入力する。そして、暗号化・復号部１７１において、ＳＡＭ管理部１９０が入力したコンテンツファイルＣＦと、キーファイルKF_1およびその署名データ$SIG_{42,SAM1}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、相互認証部１７０とＳＡＭ１０５$_1$の相互認証部１７０との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

【０１４５】次に、セッション鍵データK_{SES}を用いて復号されたキーファイルKF_1およびその署名データ$SIG_{42,SAM1}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、スタックメモリ２００に書き込まれる。

【０１４６】次に、署名処理部１８９は、スタックメモリ２００から読み出した署名データ$SIG_{22,ESC}$を、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。そして、署名処理部１８９は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データ$K_{SAM1,P}$を用いて、署名データ$SIG_{42,SAM1}$の正当を確認する。

【０１４７】次に、署名データ$SIG_{42,SAM1}$の正当性、すなわちキーファイルKF_1の作成者の正当性が確認されると、図１８（Ｂ）に示すキーファイルKF_1をスタックメモリ２００から読み出して暗号化・復号部１７３に出力する。なお、当該例では、キーファイルKF_1の作成者と送信元とが同じ場合を述べたが、キーファイルKF_1の作成者と送信元とが異なる場合には、キーファイルKF_1に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【００４８】そして、暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いてキーファイルKF_1を順に暗号化してメディアＳＡＭ管理部１９７に出力する。なお、メディア鍵データK_{MED}は、図１７に示す相互認証部１７０と図１６に示す

ＲＡＭ型の記録媒体２５０のメディアＳＡＭ２５２との間の相互認証によって記憶部１９２に事前に記憶されている。

【０１４９】ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ(Super Audio Compact Disk)、ＤＶＤ(Digital Versatile Disc)機器、ＣＤ－Ｒ機器およびＭＤ(Mini Disc)機器などの種類（当該例では、ＡＶ機器１６０$_2$）に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。なお、ＳＡＣＤとＤＶＤとでは、ディスク媒体の物理的な構造が同じであるため、ＤＶＤ機器を用いてＳＡＣＤの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。

【０１５０】また、メディア鍵データK_{MED}は、記録媒体（当該例では、ＲＡＭ型の記録媒体２５０）にユニークなデータである。メディア鍵データK_{MED}は、記録媒体（当該例では、図１６に示すＲＡＭ型の記録媒体２５０）側に格納されており、記録媒体のメディアＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアＳＡＭが搭載されている場合には、当該メディアＳＡＭ内に記憶されており、記録媒体にメディアＳＡＭが搭載されていない場合には、例えば、ＲＡＭ領域内のホストＣＰＵ８１０の管理外の領域に記憶されている。なお、本実施形態のように、機器側のＳＡＭ（当該例では、ＳＡＭ１０５$_2$）とメディアＳＡＭ（当該例では、メディアＳＡＭ２５２）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のＳＡＭに転送し、機器側のＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【０１５１】また、購入者鍵データK_{PIN}は、コンテンツファイルＣＦの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してＥＭＤサービスセンタ１０２によって割り当てられる。購入者鍵データK_{PIN}は、ＥＭＤサービスセンタ１０２において管理される。

【０１５２】メディアＳＡＭ管理部１９７は、ＳＡＭ管理部１９０から入力したコンテンツファイルＣＦおよび暗号化・復号部１７３から入力したキーファイルKF_1を、図１６に示す記録モジュール２６０に出力する。そして、記録モジュール２６０は、メディアＳＡＭ管理部１９７から入力したコンテンツファイルＣＦおよびキーファイルKF_1を、図１６に示すＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１に書き込む。この場合に、キーファイルKF_1を、メディアＳＡＭ２５２内に書き込む

ようにしてもよい。

【０１５３】次に、コンテンツの購入形態が未決定の図５に示すＲＯＭ型の記録媒体１３０をユーザホームネットワーク３０３がオフラインで配給を受けた場合に、ＡＶ機器160_2において購入形態を決定する際の処理の流れを図２０および図２１を参照しながら説明する。ＡＶ機器160_2のＳＡＭ105_2は、先ず、図２１に示す相互認証部１７０と図５に示すＲＯＭ型の記録媒体１３０のメディアＳＡＭ１３３との間で相互認証を行った後に、メディアＳＡＭ１３３からメディア鍵データK_{MED}を入力する。なお、ＳＡＭ105_2が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。次に、ＲＯＭ型の記録媒体１３０のＲＡＭ領域１３２に記録されているセキュアコンテナ１０４に格納された図４（Ｂ），（Ｃ）に示すキーファイルＫＦおよびその署名データ$ＳＩＧ_{7,CP}$と、公開鍵証明書データ$ＣＥＲ_{CP}$およびその署名データ$ＳＩＧ_{1,ESC}$とを、メディアＳＡＭ管理部１９７を介して入力し、これをスタックメモリ２００に書き込む。

【０１５４】次に、署名処理部１８９において、署名データ$ＳＩＧ_{1,ESC}$の正当性を確認した後に、公開鍵証明書データ$ＣＥＲ_{CP}$から公開鍵データ$K_{CP,P}$を取り出し、この公開鍵データ$K_{CP,P}$を用いて、署名データ$ＳＩＧ_{7,CP}$の正当性、すなわちキーファイルＫＦの作成者の正当性を検証する。

【０１５５】署名処理部１８９において署名データ$ＳＩＧ_{7,CP}$の正当性が確認されると、スタックメモリ２００からセキュアコンテナ復号部１８３に、キーファイルＫＦを読み出す。次に、セキュアコンテナ復号部１８３において、対応する期間の配信用鍵データKD_1～KD_3を用いて、キーファイルＫＦを復号する。次に、署名処理部１８９において、公開鍵データ$K_{ESC,P}$を用いて、キーファイルＫＦに格納された署名データ$ＳＩＧ_{1,ESCM}$の正当性を確認した後に、キーファイルＫＦ内の公開鍵証明書データ$ＣＥＲ_{CP}$に格納された公開鍵データ$K_{CP,P}$を用いて、署名データ$ＳＩＧ_{2,CP}$～$ＳＩＧ_{4,CP}$の正当性、すなわちコンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の作成者の正当性を検証する。

【０１５６】次に、図２１に示す相互認証部１７０と図２０に示す復号・伸長モジュール１６３との間で相互認証を行った後に、ＳＡＭ105_2の復号・伸長モジュール管理部１８４は、スタックメモリ２００に記憶されているコンテンツ鍵データＫｃおよび権利書データ１０６に格納された半開示パラメータデータ１９９、並びにＲＯＭ型の記録媒体１３０のＲＯＭ領域１３１から読み出したコンテンツデータＣを図２０に示す復号・伸長モジュール１６３に出力する。次に、復号・伸長モジュール１６３において、コンテンツデータＣがコンテンツ鍵データＫｃを用いて半開示モードで復号された後に伸長され、再生モジュール２７０に出力される。そして、再生モジュール２７０において、復号・伸長モジュール１６３からのコンテンツデータＣが再生される。

【０１５７】次に、ユーザによる図２０に示す購入形態決定操作部１６５の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号Ｓ１６５が課金処理部１８７に入力される。

【０１５８】次に、課金５８部１８７は、操作信号Ｓ１６５に応じた利用制御状態データ１６６を作成し、これをスタックメモリ２００に書き込む。次に、スタックメモリ２００から暗号化・復号部１７３に、例えば、図４（Ｂ）に示すキーファイルＫＦに利御制御状態データ１６６を格納した図１８（Ｂ）に示す新たなキーファイル$ＫＦ_1$が出力される。

【０１５９】次に、暗号化・復号部１７３は、スタックメモリ２００から読み出した図１８（Ｂ）に示すキーファイル$ＫＦ_1$を、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化してメディアＳＡＭ管理部１９７に出力する。次に、図２１に示す相互認証部１７０と図２０に示すメディアＳＡＭ１３３との間で相互認証を行った後に、ＳＡＭ管理部１９７は、暗号化・復号部１７３から入力したキーファイル$ＫＦ_1$を図２０に示す記録モジュール２７１を介してＲＯＭ型の記録媒体１３０のＲＡＭ領域１３２あるいはメディアＳＡＭ１３３内に書き込む。これにより、購入形態が決定されたＲＯＭ型の記録媒体１３０が得られる。このとき、課金処理部１８７が生成した利用制御状態データ１６６および利用履歴データ１０８は、所定のタイミングで、スタックメモリ２００および外部メモリ２０１からそれぞれ読み出しされたＥＭＤサービスセンタ１０２に送信される。

【０１６０】以下、図２２に示すように、ＡＶ機器160_3において購入形態が未決定のＲＯＭ型の記録媒体１３０からセキュアコンテナ１０４を読み出してＡＶ機器160_2に転送し、ＡＶ機器160_2において購入形態を決定してＲＡＭ型の記録媒体２５０に書き込む際の処理の流れを説明する。なお、ＲＯＭ型の記録媒体１３０からＲＡＭ型の記録媒体２５０へのセキュアコンテナ１０４の転送は、図１に示すネットワーク機器160_1およびＡＶ機器160_1～160_4のいずれの間で行ってもよい。

【０１６１】先ず、ＡＶ機器160_3のＳＡＭ105_3とＲＯＭ型の記録媒体１３０のメディアＳＡＭ１３３との間で相互認証を行い、ＲＯＭ型の記録媒体１３０のメディア鍵データK_{MED1}をＳＡＭ105_3に転送する。また、ＡＶ機器160_2のＳＡＭ105_2とＲＡＭ型の記録媒体２５０のメディアＳＡＭ２５２との間で相互認証を行い、ＲＡＭ型の記録媒体２５０のメディア鍵データK_{MED2}をＳＡＭ105_2に転送する。

67

【０１６２】次に、ＳＡＭ１０５$_3$は、ＲＯＭ型の記録媒体１３０のＲＯＭ領域１３１から読み出した図４（Ａ）に示すコンテンツファイルＣＦと、ＲＡＭ領域１３２から読み出した図４（Ｂ），（Ｃ）キーファイルＫＦ、署名データＳＩＧ$_{7,CP}$、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$とを、図２３に示す暗号化・復号部１７２において、対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて順に復号する。次に、暗号化・復号部１７２で復号されたコンテンツファイルＣＦは、暗号化・復号部１７１に出力され、ＳＡＭ１０５$_3$と１０５$_2$との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて暗号化された後に、ＳＡＭ管理部１９０に出力される。また、暗号化・復号部１７２で復号されたキーファイルＫＦは、暗号化・復号部１７１および署名処理部１８９に出力される。署名処理部１８９は、ＳＡＭ１０５$_3$の秘密鍵データＫ$_{SAM3,S}$を用いて、キーファイルＫＦの署名データＳＩＧ$_{350,SAM3}$を作成し、これを暗号化・復号部１７１に出力する。

【０１６３】また、暗号化・復号部１７１は、記憶部１９２から読み出したＳＡＭ１０５$_3$の公開鍵証明書データＣＥＲ$_{SAM3}$およびその署名データＳＩＧ$_{351,ESC}$と、キーファイルＫＦおよびその署名データＳＩＧ$_{350,SAM3}$と、暗号化・復号部１７２から入力したコンテンツファイルＣＦとを、ＳＡＭ１０５$_3$と１０５$_2$との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ＳＡＭ管理部１９０を介して、ＡＶ機器１６０$_2$のＳＡＭ１０５$_2$に出力する。

【０１６４】ＳＡＭ１０５$_2$では、図２４に示すように、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力されたコンテンツファイルＣＦが、暗号化・復号部１７１においてセッション鍵データＫ$_{SES}$を用いて復号された後に、メディアＳＡＭ管理部１９７を介してＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１に書き込まれる。

【０１６５】また、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力されたキーファイルＫＦおよびその署名データＳＩＧ$_{350,SAM3}$と、公開鍵証明書データＣＥＲ$_{SAM3}$およびその署名データＳＩＧ$_{351,ESC}$とが、スタックメモリ２００に書き込まれた後に、暗号化・復号部１７１においてセッション鍵データＫ$_{SES}$を用いて復号される。次に、当該復号された署名データＳＩＧ$_{351,ECS}$が、署名処理部１８９において署名検証され、その正当性が確認されると、公開鍵証明書データＣＥＲ$_{SAM3}$に格納された公開鍵データＫ$_{SAM3}$を用いて、署名データＳＩＧ$_{350,SAM3}$の正当性、すなわちキーファイルＫＦの送信元の正当性が確認される。そして、署名データＳＩＧ$_{350,SAM3}$の正当性が確認されると、スタックメモリ２００からキーファイルＫＦが読み出されてセキュアコンテナ復号部１８３に出力される。

68

【０１６６】次に、セキュアコンテナ復号部１８３は、対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて、キーファイルＫＦを復号し、所定の署名検証を経た後に、当該復号したキーファイルＫＦをスタックメモリ２００に書き込む。

【０１６７】次に、スタックメモリ２００に記憶されている既に復号されたキーファイルＫＦに格納された権利書データ１０６が、利用監視部１８６に出力される。利用監視部１８６は、権利書データ１０６に基づいて、コンテンツの購入形態および利用形態が管理される。

【０１６８】次に、例えば、ユーザによって試聴モードが選択されると、既にセッション鍵データＫ$_{SES}$で復号されたコンテンツファイルＣＦのコンテンツデータＣと、スタックメモリ２００に記憶されたコンテンツ鍵データＫｃ、権利書データ１０６から得られた半開示パラメータデータ１９９およびユーザ電子透かし情報用データ１９６とが、相互認証を経た後に、図２２に示す復号・伸長モジュール管理部１８４を介して再生モジュール２７０に出力される。そして、再生モジュール２７０において、試聴モードに対応したコンテンツデータＣの再生が行われる。

【０１６９】次に、ユーザによる図２２に示す購入・利用形態決定操作部１６５の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。そして、課金処理部１８７において、決定された購入・利用形態に応じて利用制御状態データ１６６および利用履歴データ１０８が生成され、これがスタックメモリ２００および外部メモリ２０１にそれぞれ書き込まれる。次に、利用制御状態データ１６６を格納した例えば図１８（Ｂ）に示すキーファイルＫＦ$_1$が、スタックメモリ２００から暗号化・復号部１７３に読み出され、暗号化・復号部１７３において記憶部１９２から読み出した記録用鍵データＫ$_{STR}$、メディア鍵データＫ$_{MED2}$および購入者鍵データＫ$_{PIN}$を用いて順に暗号化され、メディアＳＡＭ管理部１９７に出力される。キーファイルＫＦ$_1$は、図２２に示す記録モジュール２７１によってＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１あるいはメディアＳＡＭ２５２に書き込まれる。また、利用制御状態データ１６６および利用履歴データ１０８は、所定のタイミングで、ＥＭＤサービスセンタ１０２に送信される。

【０１７０】以下、ＳＡＭ１０５$_1$～１０５$_4$の実現方法について説明する。ＳＡＭ１０５$_1$～１０５$_4$の機能をハードウェアとして実現する場合は、メモリを内蔵したＡＳＩＣ型のＣＰＵを用いて、そのメモリには、図１０に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテ

69

ンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【０１７１】例えば、図１０に示す暗号化・復号部１７１などのモジュールは、例えば、処理速度の問題でハードウエアとしてＡＳＩＣ型のＣＰＵ内のＩＰコアとして実装される。クロック速度やＣＰＵコード体系などの性能によっては、暗号化・復号部１７１をソフトウェアとして実装してもよい。また、図１０に示す記憶部１９２や、図１０に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー（フラッシューＲＯＭ）が用いられ、作業用メモリとしてはＳＲＡＭなどの高速書き込み可能なメモリが用いられる。なお、その他にも、ＳＡＭ105_1～105_4に内蔵されるメモリとして、強誘電体メモリー（ＦｅＲＡＭ）を用いてもよい。また、ＳＡＭ105_1～105_4には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【０１７２】上述したように、ＳＡＭ105_1～105_4は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。ＳＡＭ105_1～105_4を搭載した機器のホストＣＰＵのバス経由で、当該ＳＡＭのＩＣ内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、ＳＡＭのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストＣＰＵが割り付けているアドレス空間内に存在しないように、当該ＳＡＭでは、ＣＰＵ側のメモリー空間を管理するＭＭＵ(Memory Magagement Unit)を用いて、搭載機器側のホストＣＰＵからは見えないアドレス空間を設定する。また、ＳＡＭ105_1～105_4は、Ｘ線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウエアＩＣＥ、ソフトウエアＩＣＥ）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがＩＣ製造後には使用できないような構造をしている。ＳＡＭ105_1～105_4自身は、ハードウエア的な構造においては、メモリを内蔵した通常のＡＳＩＣ型のＣＰＵであり、機能は当該ＣＰＵを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なＡＳＩＣ型のＣＰＵと異なる。

【０１７３】ＳＡＭ105_1～105_4の機能を全てソフトウエアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウエア処理をおこなう場合

70

と、通常のセットに搭載されているホストＣＰＵ上のソフトウエア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがＩＰコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ＩＣＥ（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（ＭｉｎｉＯＳ）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【０１７４】次に、図９に示す復号・伸長モジュール１６３について説明する。図９に示すように、復号・伸長モジュール１６３は、相互認証部２２０、復号部２２１、復号部２２２、伸長部２２３、電子透かし情報処理部２２４および半開示処理部２２５を有する。相互認証部２２０は、復号・伸長モジュール１６３がＳＡＭ105_1からデータを入力する際に、図１６に示す相互認証部１７０との間で相互認証を行ってセッション鍵データK_{SES}を生成する。

【０１７５】復号部２２１は、ＳＡＭ105_1から入力したコンテンツ鍵データＫｃ、半開示パラメータデータ１９９、ユーザ電子透かし情報用データ１９６およびコンテンツデータＣを、セッション鍵データK_{SES}を用いて復号する。そして、復号部２２１は、復号したコンテンツ鍵データＫｃおよびコンテンツデータＣを復号部２２２に出力し、復号したユーザ電子透かし情報用データ１９６を電子透かし情報処理部２２４に出力し、半開示パラメータデータ１９９を半開示処理部２２５に出力する。

【０１７６】復号部２２２は、半開示処理部２２５からの制御に基づいて、コンテンツ鍵データＫｃを用いて、コンテンツデータＣを半開示状態で復号し、復号したコンテンツデータＣを伸長部２２３に出力する。

【０１７７】伸長部２２３は、復号されたコンテンツデータＣを伸長して、電子透かし情報処理部２２４に出力する。伸長部２２３は、例えば、図４（Ａ）に示すコンテンツファイルＣＦに格納されたＡ／Ｖ伸長用ソフトウェアを用いて伸長処理を行い、例えば、ＡＴＲＡＣ３方式で伸長処理を行う。

【０１７８】電子透かし情報処理部２２４は、復号されたユーザ電子透かし情報用データ１９６に応じたユーザ電子透かし情報を、復号されたコンテンツデータＣに埋め込み、新たなコンテンツデータＣを生成する。電子透かし情報処理部２２４は、当該新たなコンテンツデータ

Ｃを再生モジュール１６９に出力する。このように、ユーザ電子透かし情報は、コンテンツデータＣを再生するときに、復号・伸長モジュール１６３において埋め込まれる。なお、本発明では、コンテンツデータＣにユーザ電子透かし情報用データ１９６を埋め込まないようにしてもよい。

【０１７９】半開示処理部２２５は、半開示パラメータデータ１９９に基づいて、例えば、コンテンツデータＣのうち復号を行わないブロックと、復号を行うブロックとを復号部２２２に指示する。また、半開示処理部２２５は、その他に、半開示パラメータデータ１９９に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【０１８０】再生モジュール１６９は、復号および伸長されたコンテンツデータＣに応じた再生を行う。

【０１８１】次に、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。図２５（Ａ）は、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{50}$が送信される。モジュールＭｏｄ$_{50}$には、モジュールＭｏｄ$_{51}$およびその秘密鍵データ$K_{CP,S}$による署名データＳＩＧ$_{CP}$が格納されている。モジュールＭｏｄ$_{51}$には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データＣＥＲ$_{CP}$と、公開鍵証明書データＣＥＲ$_{CP}$に対しての秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$と、送信するデータＤａｔａとが格納されている。このように、公開鍵証明書データＣＥＲ$_{CP}$を格納したモジュールＭｏｄ$_{50}$を、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に送信することで、ＳＡＭ１０５$_1$において署名データＳＩＧ$_{CP}$の検証を行なう際に、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$に公開鍵証明書データＣＥＲ$_{CP}$を送信する必要がなくなる。

【０１８２】図２５（Ｂ），（Ｃ）は、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図２５（Ｂ）に示すモジュールＭｏｄ$_{52}$が送信される。モジュールＭｏｄ$_{52}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データＳＩＧ$_{CP}$とが

格納されている。また、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$には、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図２５（Ｃ）に示すモジュールＭｏｄ$_{53}$が送信される。モジュールＭｏｄ$_{53}$には、コンテンツプロバイダ１０１の公開鍵証明書データＣＥＲ$_{CP}$と、その秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$とが格納されている。

【０１８３】図２５（Ｄ）は、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{54}$が送信される。モジュールＭｏｄ$_{54}$には、モジュールＭｏｄ$_{55}$およびその秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$が格納されている。モジュールＭｏｄ$_{55}$には、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データＣＥＲ$_{SAM1}$と、公開鍵証明書データＣＥＲ$_{SAM1}$に対しての秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$と、送信するデータＤａｔａとが格納されている。このように、公開鍵証明書データＣＥＲ$_{SAM1}$を格納したモジュールＭｏｄ$_{55}$を、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に送信することで、コンテンツプロバイダ１０１において署名データＳＩＧ$_{SAM1}$の検証を行なう際に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に公開鍵証明書データＣＥＲ$_{SAM1}$を送信する必要がなくなる。

【０１８４】図２５（Ｅ），（Ｆ）は、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図２５（Ｅ）に示すモジュールＭｏｄ$_{56}$が送信される。モジュールＭｏｄ$_{56}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$とが格納されている。また、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１には、ＥＭＤサービスセンタ１０２とコンテンツプロバイダ１０１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図２５（Ｆ）に示すモジュールＭｏｄ$_{57}$が送信される。モジュールＭｏｄ$_{57}$には、ＳＡＭ１０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$と、その秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$とが格納されている。

【０１８５】図２６（Ｇ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａ

73

をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{58}$が送信される。モジュールＭｏｄ$_{58}$には、モジュールＭｏｄ$_{59}$およびその秘密鍵データ$K_{CP,S}$による署名データＳＩＧ$_{CP}$が格納されている。モジュールＭｏｄ$_{59}$には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データＣＥＲ$_{CP}$と、公開鍵証明書データＣＥＲ$_{CP}$に対しての秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$と、送信するデータＤａｔａとが格納されている。

【０１８６】図２６（Ｈ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図２６（Ｈ）に示すモジュールＭｏｄ$_{60}$が送信される。モジュールＭｏｄ$_{60}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データＳＩＧ$_{CP}$とが格納されている。このとき、ＥＭＤサービスセンタ１０２にはコンテンツプロバイダ１０１の公開鍵証明書データＣＥＲ$_{CP}$は既に登録されている。

【０１８７】図２６（Ｉ）は、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{61}$が送信される。モジュールＭｏｄ$_{61}$には、モジュールＭｏｄ$_{62}$およびその秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$が格納されている。モジュールＭｏｄ$_{62}$には、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データＣＥＲ$_{SAM1}$と、公開鍵証明書データＣＥＲ$_{SAM1}$に対しての秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$と、送信するデータＤａｔａとが格納されている。

【０１８８】図２６（Ｊ）は、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図２６

74

（Ｊ）に示すモジュールＭｏｄ$_{63}$が送信される。モジュールＭｏｄ$_{63}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$とが格納されている。このとき、ＥＭＤサービスセンタ１０２にはＳＡＭ１０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$は既に登録されている。以下、ＳＡＭ１０５$_1$～１０５$_4$の出荷時におけるＥＭＤサービスセンタ１０２への登録処理について説明する。なお、ＳＡＭ１０５$_1$～１０５$_4$の登録処理は同じであるため、以下、ＳＡＭ１０５$_1$の登録処理について述べる。ＳＡＭ１０５$_1$の出荷時には、図８に示すＥＭＤサービスセンタ１０２の鍵サーバ１４１によって、ＳＡＭ管理部１４９を介して、図１０などに示す記憶部１９２に以下に示す鍵データが初期登録される。また、ＳＡＭ１０５$_1$には、例えば、出荷時に、記憶部１９２などに、ＳＡＭ１０５$_1$がＥＭＤサービスセンタ１０２に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部１９２には、例えば、図１４において左側に「＊」が付されているＳＡＭ１０５$_1$の識別子ＳＡＭ＿ＩＤ、記録用鍵データK_{STR}、ルート認証局２の公開鍵データK_{R-CA}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$、公開鍵証明書データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22,ESC}$、復号・伸長モジュール１６３およびメディアＳＡＭとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データＣＥＲ$_{SAM1}$は、ＳＡＭ１０５$_1$を出荷後に登録する際にＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$に送信してもよい。

【０１８９】ここで、ルート認証局２の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているＲＳＡを使用し、データ長は例えば１０２４ビットである。公開鍵データK_{R-CA}は、図１に示すルート認証局２によって発行される。また、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$は、短いデータ長でＲＳＡと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば１６０ビットである。但し、暗号化の強度を考慮すると、公開鍵データ$K_{ESC,P}$は１９２ビット以上であることが望ましい。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２に公開鍵データ$K_{ESC,P}$を登録する。また、ルート認証局９２は、公開鍵データ$K_{ESC,P}$の公開鍵証明書データＣＥＲ$_{ESC}$を作成する。公開鍵データ$K_{ESC,P}$を格納した公開鍵証明書データＣＥＲ$_{ESC}$は、好ましくＳＡＭ１０５$_1$の出荷時に記憶部１９２に記憶される。この場合に、公開鍵証明書データＣＥＲ$_{ESC}$は、ルート認証局９２の秘密鍵データ$K_{ROOT,S}$で署名されている。

【０１９０】ＥＭＤサービスセンタ１０２は、乱数を発生してＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$を生成

し、これとペアとなる公開鍵データ$K_{SAM1,P}$を生成する。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２の認証をもらって、公開鍵データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を発行し、これに自らの秘密鍵データ$K_{ESC,S}$を用いて署名データを添付する。すなわち、ＥＭＤサービスセンタ１０２は、セカンドＣＡ（認証局）として機能を果たす。

【０１９１】また、ＳＡＭ１０５$_1$には、図８に示すＥＭＤサービスセンタ１０２のＳＡＭ管理部１４９により、ＥＭＤサービスセンタ１０２の管理下にある一意（ユニーク）な識別子ＳＡＭ＿ＩＤが割り当てられ、これがＳＡＭ１０５$_1$の記憶部１９２に格納されると共に、図８に示すＳＡＭデータベース１４９ａにも格納され、ＥＭＤサービスセンタ１０２によって管理される。

【０１９２】また、ＳＡＭ１０５$_1$は、出荷後、例えば、ユーザによってＥＭＤサービスセンタ１０２と接続され、登録手続を行うと共に、ＥＭＤサービスセンタ１０２から記憶部１９２に配信用鍵データKD_1～KD_3が転送される。すなわち、ＳＡＭ１０５$_1$を利用するユーザは、コンテンツをダウンロードする前にＥＭＤサービスセンタ１０２に登録手続が必要である。この登録手続は、例えば、ＳＡＭ１０５$_1$を搭載している機器（当該例では、ネットワーク機器１６０$_1$）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。ＳＡＭ１０５$_1$は、上述した登録手続を経た後でないと使用できない。

【０１９３】ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$のユーザによる登録手続に応じて、ユーザに固有の識別子ＵＳＥＲ＿ＩＤを発行し、例えば、図８に示すＳＡＭデータベース１４９ａにおいて、ＳＡＭ＿ＩＤとＵＳＥＲ＿ＩＤとの対応関係を管理し、課金時に利用する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$のユーザに対して情報参照用識別子ＩＤと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子ＩＤとパスワードとを用いて、ＥＭＤサービスセンタ１０２に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。また、ＥＭＤサービスセンタ１０２は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【０１９４】次に、図１４に示すように、ＳＡＭ１０５$_1$内の記憶部１９２にＳＡＭ登録リストを格納する手順について説明する。図１に示すＳＡＭ１０５$_1$は、例えば、バス１９１としてＩＥＥＥ１３９４シリアルバスを用いた場合に、バス１９１に接続された機器の電源を立ち上げたり、新しい機器をバス１９１に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するＳＡＭ１０５$_2$～ＳＡＭ１０５$_4$のＳＡＭ登録リストを得る。なお、ＩＥＥＥ１３９４シリアルバスであるバス１９１に応じて生成されたトポロジーマップは、例えば、図２７に示すように、バス１９１にＳＡＭ１０５$_1$～１０５$_4$に加えてＡＶ機器１６０$_5$，１６０$_6$のＳＣＭＳ処理回路１０５$_5$，１０５$_6$が接続されている場合に、ＳＡＭ１０５$_1$～１０５$_4$およびＳＣＭＳ処理回路１０５$_5$，１０５$_6$を対象として生成される。従って、ＳＡＭ１０５$_1$は、当該トポロジーマップから、ＳＡＭ１０５$_1$～１０５$_4$についての情報を抽出してＳＡＭ登録リストを生成する。

【０１９５】ＳＡＭ登録リストのデータフォーマットは、例えば、図２８に示される。そして、ＳＡＭ１０５$_1$は、当該ＳＡＭ登録リストを、ＥＭＤサービスセンタ１０２に登録して署名を得る。これらの処理は、バス１９１のセッションを利用してＳＡＭ１０５$_1$が自動的に行い、ＥＭＤサービスセンタ１０２にＳＡＭ登録リストの登録命令を発行する。ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$から図２８に示すＳＡＭ登録リストを受けると、有効期限を確認する。そして、ＥＭＤサービスセンタ１０２は、登録時にＳＡＭ１０５$_1$より指定された決済機能の有無を参照して対応する部分の設定を行う。また、ＥＭＤサービスセンタ１０２は、リボケーションリストをチェックしてＳＡＭ登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にＥＭＤサービスセンタ１０２によって使用が禁止されている（無効な）ＳＡＭのリストである。また、ＥＭＤサービスセンタ１０２は、決済時にはＳＡＭ１０５$_1$に対応するＳＡＭ登録リストを取り出し、その中に記述されたＳＡＭがリボケーションリストに含まれているかを確認する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ登録リストに署名を添付する。なお、ＳＡＭリボケーションリストは、同一系の（同一のバス１９１に接続されている）ＳＡＭのみを対象として生成され、各ＳＡＭに対応するリボケーションンフラグによって、当該ＳＡＭの有効および無効を示している。

【０１９６】以下、図１に示すコンテンツプロバイダ１０１の全体動作について説明する。図２９は、コンテンツプロバイダ１０１の全体動作のフローチャートである。

ステップＳ１：ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１が所定の登録処理を経た後に、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をコンテンツプロバイダ１０１に送信する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$～１０５$_4$が所定の登録処理を経た後に、ＳＡＭ１０５$_1$～１０５$_4$の公開鍵データ$K_{SAM1,P}$～$K_{SAM4,P}$の公開鍵証明書CER_{CP1}～CER_{CP4}をＳＡＭ１０５$_1$～１０５$_4$に送信する。また、ＥＭＤサービスセンタ１０２は、相互認証を行った後に、各々有効期限が１カ

77

月の６カ月分の配信用鍵データKD_1～KD_6をコンテンツプロバイダ１０１に送信し、３カ月分の配信用鍵データKD_1～KD_3をユーザホームネットワーク１０３に送信する。このように、ＥＭＤシステム１００では、配信用鍵データKD_1～KD_3を予めＳＡＭ105_1～105_4に配給しているため、ＳＡＭ105_1～105_4とＥＭＤサービスセンタ１０２との間がオフラインの状態でも、ＳＡＭ105_1～105_4においてコンテンツプロバイダ１０１から配給されたセキュアコンテナ１０４を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ１０８に記述され、利用履歴データ１０８は、ＳＡＭ105_1～105_4とＥＭＤサービスセンタ１０２とが接続されたときに、ＥＭＤサービスセンタ１０２に自動的に送信されるため、ＥＭＤサービスセンタ１０２における決済処理を確実に行うことができる。なお、ＥＭＤサービスセンタ１０２が、所定の期間内に、利用履歴データ１０８を回収できないＳＡＭについては、リボケーションリストで無効の対象とする。なお、利用制御状態データ１６６は、原則として、リアルタイムで、ＳＡＭ105_1～105_4からＥＭＤサービスセンタ１０２に送信される。

【０１９７】ステップＳ２：コンテンツプロバイダ１０１は、相互認証を行った後に、図６（Ａ）に示す権利登録要求モジュールMod_2を、ＥＭＤサービスセンタ１０２に送信する。そして、ＥＭＤサービスセンタ１０２は、所定の署名検証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化する。

【０１９８】ステップＳ３：コンテンツプロバイダ１０１は、対応する期間の配信用鍵データKD_1～KD_6などを用いて暗号化を行って、図４（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびキーファイルＫＦを作成し、これらと図４（Ｃ）に示す公開鍵証明書データCER_{cp}とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、ユーザホームネットワーク１０３に配給する。

【０１９９】ステップＳ４：ユーザホームネットワーク１０３のＳＡＭ105_1～ＳＡＭ105_4は、セキュアコンテナ１０４を対応する期間の配信用鍵データKD_1～KD_3などを用いて復号し、セキュアコンテナ１０４の作成者および送信者と正当性を検証するための署名検証などを行い、セキュアコンテナ１０４が正当なコンテンツプロバイダ１０１から送信されたか否かを確認する。

【０２００】ステップＳ５：ＳＡＭ105_1～ＳＡＭ105_4において、ユーザによる図９に示す購入・利用形態決定操作部１６５の操作に応じた操作信号Ｓ１６５に基づいて、購入・利用形態を決定する。このとき、図１５に示す利用監視部１８６において、セキュアコンテナ１０４に格納された権利書データ１０６に基づいて、ユーザによるコンテンツファイルＣＦの購入・利用形態が

78

管理される。

【０２０１】ステップＳ６：ＳＡＭ105_1～ＳＡＭ105_4の図１５に示す課金処理部１８７において、操作信号Ｓ１６５に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ１０８および利用制御状態データ１６６が生成し、これらをＥＭＤサービスセンタ１０２に送信する。

【０２０２】ステップＳ７：ＥＭＤサービスセンタ１０２は、図８に示す決算処理部１４２において、利用履歴データ１０８に基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を作成する。ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データSIG_{99}を、図１に示すペイメントゲートウェイ９０を介して、決済機関９１に送信する。また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０２０３】ステップＳ８：　決済機関９１において、署名データSIG_{99}の検証を行った後に、決済請求権データ１５２に基づいて、ユーザが支払った金額が、コンテンツプロバイダ１０１の所有者に分配される。

【０２０４】第１実施形態の第１変形例

上述した実施形態では、図４（Ｂ）に示すように、コンテンツプロバイダ１０１において配信用鍵データＫＤを用いてキーファイルＫＦを暗号化し、ＳＡＭ105_1～105_4において配信用鍵データＫＤを用いてキーファイルＫＦを復号する場合を例示したが、図１に示すように、コンテンツプロバイダ１０１からＳＡＭ105_1～105_4にセキュアコンテナ１０４を直接供給する場合には、配信用鍵データＫＤを用いたキーファイルＫＦの暗号化は必ずしも行なわなくてもよい。このように、配信用鍵データＫＤを用いてキーファイルＫＦを暗号化することは、後述する第２実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データＫＤをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。但し、上述した第１実施形態の場合でも、配信用鍵データＫＤを用いてキーファイルＫＦを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【０２０５】また、上述した実施形態では、図４（Ｂ）に示すキーファイルＫＦ内の権利書データ１０６内に標準小売価格データＳＲＰを格納する場合を例示したが、セキュアコンテナ１０４内のキーファイルＫＦの外に、標準小売価格データＳＲＰ（プライスタグデータ）を格納してもよい。この場合には、標準小売価格データＳＲＰに対して秘密鍵データK_{cp}を用いて作成した署名データを添付する。

【０２０６】第１実施形態の第２変形例
上述した第１実施形態では、図１に示すように、ＥＭＤサービスセンタ１０２が、自らが生成した決済請求権データ１５２を用いて、ペイメントゲートウェイ９０を介して決済機関９１で決済処理を行なう場合を例示したが、例えば、図３０に示すように、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に決済請求権データ１５２を送信し、コンテンツプロバイダ１０１自らが、決済請求権データ１５２を用いて、ペイメントゲートウェイ９０を介して決済機関９１に対して決済処理を行なってもよい。

【０２０７】第１実施形態の第３変形例
上述した第１実施形態では、単数のコンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ105_1～105_4に、セキュアコンテナ１０４を供給する場合を例示したが、２以上のコンテンツプロバイダ１０１ａ，１０１ｂからＳＡＭ105_1～105_4にそれぞれセキュアコンテナ１０４ａ，１０４ｂを供給するようにしてもよい。図３１は、コンテンツプロバイダ１０１ａ，１０１ｂを用いる場合の第１実施形態の第２変形例に係わるＥＭＤシステムの構成図である。この場合には、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１ａおよび１０１ｂに、それぞれ６カ月分の配信用鍵データKDa_1～KDa_6およびKDb_1～KDb_6を配信する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ105_1～105_4に、３カ月分の配信用鍵データKDa_1～KDa_3およびKDb_1～KDb_3を配信する。

【０２０８】そして、コンテンツプロバイダ１０１ａは、独自のコンテンツ鍵データＫｃａを用いて暗号化したコンテンツファイルＣＦａと、コンテンツ鍵データＫｃａおよび権利書データ１０６ａなどを対応する期間の配信用鍵データKDa_1～KDa_6を用いて暗号化したキーファイルＫＦａとを格納したセキュアコンテナ１０４ａをＳＡＭ105_1～105_4にオンラインおよび／またはオフランで供給する。このとき、キーファイルの識別子として、ＥＭＤサービスセンタ１０２が配付するグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤが用いられ、ＥＭＤサービスセンタ１０２によって、コンテンツデータが一元的に管理される。また、コンテンツプロバイダ１０１ｂは、独自のコンテンツ鍵データＫｃｂを用いて暗号化したコンテンツファイルＣＦｂと、コンテンツ鍵データＫｃｂおよび権利書データ１０６ｂなどを対応する期間の配信用鍵データKDb_1～KDb_6を用いて暗号化したキーファイルＫＦｂとを格納したセキュアコンテナ１０４ｂをＳＡＭ105_1～105_4にオンラインおよび／またはオフランで供給する。

【０２０９】ＳＡＭ105_1～105_4は、セキュアコンテナ１０４ａについては、対応する期間の配信用鍵データKDa_1～KDa_3を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ１０８ａおよび利用制御状態データ１６６ａをＥＭＤサービスセンタ１０２に送信する。また、ＳＡＭ105_1～105_4は、セキュアコンテナ１０４ｂについては、対応する期間の配信用鍵データKDb_1～KDb_3を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ１０８ｂおよび利用制御状態データ１６６ｂをＥＭＤサービスセンタ１０２に送信する。

【０２１０】ＥＭＤサービスセンタ１０２では、利用履歴データ１０８ａに基づいて、コンテンツプロバイダ１０１ａについての決済請求権データ１５２ａを作成し、これを用いて決済機関９１に対して決済処理を行なう。また、ＥＭＤサービスセンタ１０２では、利用履歴データ１０８ｂに基づいて、コンテンツプロバイダ１０１ｂについての決済請求権データ１５２ｂを作成し、これを用いて決済機関９１に対して決済処理を行なう。

【０２１１】また、ＥＭＤサービスセンタ１０２は、権利書データ１０６ａ，１０６ｂを登録して権威化を行なう。このとき、ＥＭＤサービスセンタ１０２は、権利書データ１０６ａ，１０６ｂに対応するキーファイルＫＦａ，ＫＦｂに対して、グローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤを配付する。また、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１ａ，１０１ｂの公開鍵証明書データCER_{cpa}，CER_{CPb}を発行し、これに自らの署名データ$SIG_{1b,ESC}$，$SIG_{1a,ESC}$を付してその正当性を認証する。

【０２１２】第２実施形態
上述した実施形態では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ105_1～105_4にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのＳＡＭに配給する場合について説明する。

【０２１３】図３２は、本実施形態のＥＭＤシステム３００の構成図である。図３２に示すように、ＥＭＤシステム３００は、コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ユーザホームネットワーク３０３、サービスプロバイダ３１０、ペイメントゲートウェイ９０および決済機関９１を有する。コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ＳＡＭ3051_1～3054_4などおよびサービスプロバイダ３１０は、それぞれ請求項２２などに係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置にそれぞれ対応している。コンテンツプロバイダ３０１は、サービスプロバイダ３１０に対してコンテンツデータを供給する点を除いて、前述した第１実施形態のコンテンツ

81

プロバイダ１０１と同じである。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ１０１およびＳＡＭ５０５$_1$～５０５$_4$に加えて、サービスプロバイダ３１０に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第１実施形態のＥＭＤサービスセンタ１０２と同じである。また、ユーザホームネットワーク３０３は、ネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$を有している。ネットワーク機器３６０$_1$はＳＡＭ３０５$_1$およびＣＡモジュール３１１を内蔵しており、ＡＶ機器３６０$_2$～３６０$_4$はそれぞれＳＡＭ３０５$_2$～３０５$_4$を内蔵している。ここで、ＳＡＭ３０５$_1$～３０５$_4$は、サービスプロバイダ３１０からセキュアコンテナ３０４の配給を受ける点と、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０についての署名データの検証処理およびＳＰ用購入履歴データ（データ配給装置用購入履歴データ）３０９の作成を行なう点とを除いて、前述した第１実施形態のＳＡＭ１０５$_1$～１０５$_4$と同じである。

【０２１４】先ず、ＥＭＤシステム３００の概要について説明する。ＥＭＤシステム３００では、コンテンツプロバイダ３０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す前述した第１実施形態と同様の権利書(UCP:Usage Control Policy)データ１０６を、高い信頼性のある権威機関であるＥＭＤサービスセンタ３０２に送信する。権利書データ１０６は、ＥＭＤサービスセンタ３０２に登録されて権威化（認証）される。

【０２１５】また、コンテンツプロバイダ３０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成する。また、コンテンツプロバイダ３０１は、ＥＭＤサービスセンタ３０２から配給された対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_6$を用いて、コンテンツ鍵データＫｃおよび権利書データ１０６を暗号化し、それらを格納したキーファイルＫＦを作成する。そして、コンテンツプロバイダ３０１は、コンテンツファイルＣＦ、キーファイルＫＦおよび自らの署名データとを格納したセキュアコンテナ１０４を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ３１０に供給する。

【０２１６】サービスプロバイダ３１０は、コンテンツプロバイダ３０１からセキュアコンテナ１０４を受け取ると、署名データの検証を行なって、セキュアコンテナ１０４が正当なコンテンツプロバイダ３０１によって作成されたものであるか、並びに送り主の正当性を確認する。次に、サービスプロバイダ３１０は、例えばオフラインで通知されたコンテンツプロバイダ３０１が希望するコンテンツに対しての価格（ＳＲＰ）に、自らのサービスの価格を加算した価格を示すプライスタグデータ（ＰＴ）３１２を作成する。そして、サービスプロバイダ３１０は、セキュアコンテナ１０４から取り出したコンテンツファイルＣＦおよびキーファイルＫＦと、プライスタグデータ３１２と、これらに対しての自らの秘密鍵データ$K_{SP,S}$による署名データとを格納したセキュアコンテナ３０４を作成する。このとき、キーファイルＫＦは、配信用鍵データＫＤ$_1$～ＫＤ$_6$によって暗号化されており、サービスプロバイダ３１０は当該配信用鍵データＫＤ$_1$～ＫＤ$_6$を保持していないため、サービスプロバイダ３１０はキーファイルＫＦの中身を見たり、書き換えたりすることはできない。また、ＥＭＤサービスセンタ３０２は、プライスタグデータ３１２を登録して権威化する。

【０２１７】サービスプロバイダ３１０は、オンラインおよび／またはオフラインでセキュアコンテナ３０４をユーザホームネットワーク３０３に配給する。このとき、オフラインの場合には、セキュアコンテナ３０４はＳＡＭ３０５$_1$～３０５$_4$にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ３１０とＣＡモジュール３１１との間で相互認証を行い、セキュアコンテナ３０４をサービスプロバイダ３１０においてセッション鍵データK_{SES}を用いた暗号化して送信し、ＣＡモジュール３１１において受信したセキュアコンテナ３０４をセッション鍵データK_{SES}を用いて復号した後に、ＳＡＭ３０５$_1$～３０５$_4$に転送する。

【０２１８】次に、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４を、ＥＭＤサービスセンタ３０２から配給された対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて復号した後に、署名データの検証処理を行う。ＳＡＭ３０５$_1$～３０５$_4$に供給されたセキュアコンテナ３０４は、ネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。ＳＡＭ３０５$_1$～３０５$_4$は、上述したセキュアコンテナ３０４の購入・利用の履歴を利用履歴(Usage Log) データ３０８として記録する。利用履歴データ（履歴データまたは管理装置用履歴データ）３０８は、例えば、ＥＭＤサービスセンタ３０２からの要求に応じて、ユーザホームネットワーク３０３からＥＭＤサービスセンタ３０２に送信される。

【０２１９】ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１およびサービスプロバイダ３１０に分配され

82

る。

【０２２０】本実施形態では、ＥＭＤサービスセンタ３０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、ＥＭＤサービスセンタ３０２は、中立の立場にある最高の権威機関であるルート認証局９２に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ305_1～305_4において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ３０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ３０１の権利書データ１０６およびサービスプロバイダ３１０のプライスタグデータ３１２を登録して権威化することも、ＥＭＤサービスセンタ３０２の認証機能によるものである。また、ＥＭＤサービスセンタ３０２は、例えば、配信用鍵データKD_1～KD_6などの鍵データの管理を行なう鍵データ管理機能を有する。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１が登録した権利書データ１０６とＳＡＭ3051_1～ＳＡＭ3054_4から入力した利用履歴データ３０８とサービスプロバイダ３１０が登録したプライスタグデータ３１２とに基づいて、ユーザホームネットワーク３０３のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ３０１およびサービスプロバイダ３１０に分配して支払う権利処理（利益分配）機能を有する。

【０２２１】以下、コンテンツプロバイダ３０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ３０１〕図３３は、コンテンツプロバイダ３０１の機能ブロック図であり、サービスプロバイダ３１０との間で送受信されるデータに関連するデータの流れが示されている。図３３に示すように、コンテンツプロバイダ３０１は、コンテンツマスタソースサーバ１１１、電子透かし情報付加部１１２、圧縮部１１３、暗号化部１１４、乱数発生部１１５、暗号化部１１６、署名処理部１１７、セキュアコンテナ作成部１１８、セキュアコンテナデータベース１１８ａ、記憶部１１９、相互認証部１２０、暗号化・復号部１２１、権利書データ作成部１２２、ＥＭＤサービスセンタ管理部１２５およびサービスプロバイダ管理部３２４を有する。

【０２２２】図３３において、図２と同一符号を付した構成要素は、前述した第１実施形態において図２および図３を参照しながら説明した同一符号の構成要素と同じである。すなわち、コンテンツプロバイダ３０１は、図２に示すＳＡＭ管理部１２４の代わりにサービスプロバイダ管理部３２４を設けた構成をしている。サービスプロバイダ管理部３２４は、セキュアコンテナ作成部１１８から入力したセキュアコンテナ１０４を、オフラインおよび／またはオンラインで、図３２に示すサービスプロバイダ３１０に提供する。セキュアコンテナ１０４には、第１実施形態と同様に、図４（Ａ），（Ｂ），（Ｃ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$とが格納されている。

【０２２３】サービスプロバイダ管理部３２４は、セキュアコンテナ１０４をオンラインでサービスプロバイダ３１０に配信する場合には、暗号化・復号部１２１においてセッション鍵データK_{SES}を用いてセキュアコンテナ１０４を暗号化した後に、ネットワークを介してサービスプロバイダ３１０に配信する。

【０２２４】また、図３に示すしたコンテンツプロバイダ１０１内でのデータの流れは、サービスプロバイダ３１０にも同様に適用される。

【０２２５】〔サービスプロバイダ３１０〕サービスプロバイダ３１０は、コンテンツプロバイダ３０１から提供を受けたセキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦと、自らが生成したプライスタグデータ３１２とを格納したセキュアコンテナ３０４を、オンラインおよび／またはオフラインで、ユーザホームネットワーク３０３のネットワーク機器3601_1およびＡＶ機器3602_2～3604_4に配給する。サービスプロバイダ３１０によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、ＣＭ（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【０２２６】図３４は、サービスプロバイダ３１０の機能ブロック図である。なお、図３４には、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４に応じたセキュアコンテナ３０４をユーザホームネットワーク３０３に供給する際のデータの流れが示されている。図３４に示すように、サービスプロバイダ３１０は、コンテンツプロバイダ管理部３５０、記憶部３５１、相互認証部３５２、暗号化・復号部３５３、署名処理部３５４、セキュアコンテナ作成部３５５、セキュアコンテナデータベース３５５ａ、プライスタグデータ作成部３５６、ユーザホームネットワーク管理部３５７、ＥＭＤサービスセンタ管理部３５８およびユーザ嗜好フィルタ生成部９２０を有する。

【０２２７】以下、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４からセキュアコンテナ３０４を作成し、これをユーザホームネットワーク３

85

０３に配給する際のサービスプロバイダ３１０内での処理の流れを図３４を参照しながら説明する。コンテンツプロバイダ管理部３５０は、オンラインおよび／またはオフラインで、コンテンツプロバイダ３０１から図４に示すセキュアコンテナ１０４の供給を受けてセキュアコンテナ１０４を記憶部３５１に書き込む。このとき、コンテンツプロバイダ管理部３５０は、オンラインの場合には、図３３に示す相互認証部１２０と図３４に示す相互認証部３５２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテナ１０４を暗号化・復号部３５３において復号した後に、記憶部３５１に書き込む。

【０２２８】次に、署名処理部３５４において、記憶部３５１に記憶されているセキュアコンテナ１０４の図４（Ｃ）に示す署名データ$SIG_{1,ESC}$を、記憶部３５１から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$を用いて検証し、その正当性が認められた後に、図４（Ｃ）に示す公開鍵証明書データCER_{CP}から公開鍵データ$K_{CP,P}$を取り出す。次に、署名処理部３５４は、当該取り出した公開鍵データ$K_{CP,P}$を用いて、記憶部３５１に記憶されているセキュアコンテナ１０４の図４（Ａ），（Ｂ）に示す署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の検証を行う。

【０２２９】次に、セキュアコンテナ作成部３５５は、署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の正当性が確認されると、記憶部３５１からコンテンツファイルＣＦと、キーファイルＫＦと、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$とを読み出す。

【０２３０】また、プライスタグデータ作成部３５６は、例えばコンテンツプロバイダ３０１からオフラインで通知されたコンテンツプロバイダ３０１が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ３１２を作成し、これをセキュアコンテナ作成部３５５に出力する。

【０２３１】また、署名処理部３５４は、コンテンツファイルＣＦ、キーファイルＫＦおよびプライスタグデータ３１２のハッシュ値をとり、サービスプロバイダ３１０の秘密鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$を作成し、これをセキュアコンテナ作成部３５５に出力する。

【０２３２】次に、セキュアコンテナ作成部３５５は、図３５（Ａ）～（Ｄ）に示すように、コンテンツファイルＣＦおよびその署名データ$SIG_{62,SP}$と、キーファイルＫＦおよびその署名データ$SIG_{63,ESC}$と、プライスタグデータ３１２およびその署名データ$SIG_{64,SP}$と、公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$とを格納したセキュアコンテナ３０４を作成し、セキュアコンテナデータベース３５５ａに格納する。そして、セキュアコンテナ作成部３５５は、ユーザ

86

ホームネットワーク３０３からの要求に応じたセキュアコンテナ３０４をセキュアコンテナデータベース３５５ａから読み出してユーザホームネットワーク管理部３５７に出力する。このとき、セキュアコンテナ３０４は、複数のコンテンツファイルＣＦと、それらにそれぞれ対応した複数のキーファイルＫＦとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ３０４内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルＣＦを単数のセキュアコンテナ３０４に格納してもよい。これらの複数のコンテンツファイルＣＦなどは、ディレクトリー構造でセキュアコンテナ３０４内に格納してもよい。

【０２３３】また、セキュアコンテナ３０４は、デジタル放送で送信される場合には、ＭＨＥＧ(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはＸＭＬ／ＳＭＩＬ／ＨＴＭＬ(Hyper TextMarkup Language) プロトコルが用いられる。このとき、コンテンツファイルＣＦおよびキーファイルＫＦは、コンテンツプロバイダ３０１によって一元的に管理され、セキュアコンテナ３０４を送信するプロトコルに依存しない。すなわち、コンテンツファイルＣＦおよびキーファイルＫＦは、ＭＨＥＧおよびＨＴＭＬのプロコトルをトンネリングした形でセキュアコンテナ３０４内に格納される。

【０２３４】次に、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４を、オフラインおよび／またはオンラインでユーザホームネットワーク３０３に供給する。ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４をオンラインでユーザホームネットワーク３０３のネットワーク機器360_1に配信する場合には、相互認証後に、暗号化・復号部３５２においてセッション鍵データK_{SES}を用いてセキュアコンテナ３０４を暗号化した後に、ネットワークを介してネットワーク機器360_1に配信する。

【０２３５】なお、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４を例えば衛星などを介して放送する場合には、セキュアコンテナ３０４をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}をワーク鍵データK_Wを暗号化し、ワーク鍵データK_Wをマスタ鍵データK_Mを用いて暗号化する。そして、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４と共に、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを、衛星を介してユーザホームネットワーク３０３に送信する。また、例えば、マスタ鍵データK_Mを、ＩＣカードなどに記憶してオフラインでユーザホームネットワーク３０３に配給する。

【０２３６】また、ユーザホームネットワーク管理部３５７は、ユーザホームネットワーク３０３から、当該サ

ービスプロバイダ３１０が配給したコンテンツデータＣに関してのＳＰ用購入履歴データ３０９を受信すると、これを記憶部３５１に書き込む。サービスプロバイダ３１０は、将来のサービス内容を決定する際に、ＳＰ用購入履歴データ３０９を参照する。また、ユーザ嗜好フィルタ生成部９２０は、ＳＰ用購入履歴データ３０９に基づいて、当該ＳＰ用購入履歴データ３０９を送信した$SAM305_1$～305_4のユーザの嗜好を分析してユーザ嗜好フィルタデータ９００を生成し、これをユーザホームネットワーク管理部３５７を介してユーザホームネットワーク３０３のＣＡモジュール３１１に送信する。

【０２３７】図３６には、サービスプロバイダ３１０内におけるＥＭＤサービスセンタ３０２との間の通信に関連するデータの流れが示されている。なお、以下に示す処理を行う前提として、サービスプロバイダ３１０の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ３０２に登録処理を行い、グローバルユニークな識別子ＳＰ＿ＩＤを得ている。識別子ＳＰ＿ＩＤは、記憶部３５１に記憶される。

【０２３８】先ず、サービスプロバイダ３１０が、ＥＭＤサービスセンタ３０２に、自らの秘密鍵データ$K_{SP,S}$に対応する公開鍵データ$K_{SP,S}$の正当性を証明する公開鍵証明書データCER_{SP}を要求する場合の処理を図３６を参照しながら説明する。先ず、サービスプロバイダ３１０は、真性乱数発生器を用いて乱数を発生して秘密鍵データ$K_{SP,S}$を生成し、当該秘密鍵データ$K_{SP,S}$に対応する公開鍵データ$K_{SP,P}$を作成して記憶部３５１に記憶する。ＥＭＤサービスセンタ管理部３５８、サービスプロバイダ３１０の識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$を記憶部３５１から読み出す。そして、ＥＭＤサービスセンタ管理部３５８は、識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$を、ＥＭＤサービスセンタ３０２に送信する。そして、ＥＭＤサービスセンタ管理部３４８は、当該登録に応じて、公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$をＥＭＤサービスセンタ３０２から入力して記憶部３５１に書き込む。

【０２３９】次に、サービスプロバイダ３１０が、ＥＭＤサービスセンタ３０２にプライスタグデータ３１２を登録して権威化する場合の処理を図３６を参照して説明する。

【０２４０】この場合には、署名処理部３５４において、プライスタグデータ作成部３５６が作成したプライスタグデータ３１２と記憶部３５１から読み出したグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤとを格納したモジュールMod_{103}のハッシュ値が求められ、秘密鍵データ$K_{SP,S}$を用いて署名データ$SIG_{80,SP}$が生成される。また、記憶部３５１から公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$が読み出される。そして、図３７に示すプライスタグ登録要求用モジュールMod_{102}を、相互認証部３５２とＥＭＤサービスセンタ３０２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部３５３において暗号化した後に、ＥＭＤサービスセンタ管理部３５８からＥＭＤサービスセンタ３０２に送信する。なお、モジュールMod_{103}に、サービスプロバイダ３１０のグローバルユニークな識別子ＳＰ＿ＩＤを格納してもよい。

【０２４１】また、ＥＭＤサービスセンタ管理部３５８は、ＥＭＤサービスセンタ３０２から受信した決済レポートデータ３０７ｓを記憶部３５１に書き込む。

【０２４２】また、ＥＭＤサービスセンタ管理部３５８は、ＥＭＤサービスセンタ３０２から受信したマーケティング情報データ９０４を記憶部３５１に記憶する。マーケティング情報データ９０４は、サービスプロバイダ３１０が今後配給するコンテンツデータＣを決定する際に参考にされる。

【０２４３】〔ＥＭＤサービスセンタ３０２〕ＥＭＤサービスセンタ３０２は、前述したように、認証局（ＣＡ:CertificateAuthority）、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。図３８は、ＥＭＤサービスセンタ３０２の機能の構成図である。図３８に示すように、ＥＭＤサービスセンタ３０２は、鍵サーバ１４１、鍵データベース１４１ａ、決済処理部４４２、署名処理部４４３、決算機関管理部１４４、証明書・権利書管理部４４５、ＣＥＲデータベース４４５ａ、コンテンツプロバイダ管理部１４８、ＣＰデータベース１４８ａ、ＳＡＭ管理部１４９、ＳＡＭデータベース１４９ａ、相互認証部１５０、暗号化・復号部１５１、サービスプロバイダ管理部３９０、ＳＰデータベース３９０ａ、ユーザ嗜好フィルタ生成部９０１およびマーケティング情報データ生成部９０２を有する。図３８において、図７および図８と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。以下、図３８において、新たな符号を付した機能ブロックについて説明する。なお、図３８には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ３１０との間で送受信されるデータに関連するデータの流れが示されている。また、図３９には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ３０１との間で送受信されるデータに関連するデータの流れが示されている。また、図４０には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、図３２に示す$SAM305_1$～305_4および決済機関９１との間で送受信されるデータに関連するデータの流れが示されている。

【０２４４】決算処理部４４２は、図４０に示すように、$SAM305_1$～305_4から入力した利用履歴デ

89

ータ３０８と、証明書・権利書管理部４４５から入力した標準小売価格データＳＲＰおよびプライスタグデータ３１２に基づいて決済処理を行う。なお、この際に、決済処理部４４２は、サービスプロバイダ３１０によるダンピングの有無などを監視する。決済処理部４４２は、決済処理により、図４０に示すように、コンテンツプロバイダ３０１についての決済レポートデータ３０７ｃおよび決済請求権データ１５２ｃを作成し、これらをそれぞれコンテンツプロバイダ管理部１４８および決算機関管理部１４４に出力する。また、決済処理により、図３８および図４０に示すように、サービスプロバイダ３１０についての決済レポートデータ３０７ｓおよび決済請求権データ１５２ｓを作成し、これらをそれぞれサービスプロバイダ管理部３９０および決算機関管理部１４４に出力する。ここで、決済請求権データ１５２ｃ，１５２ｓは、当該データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータである。

【０２４５】ここで、利用履歴データ３０８は、第１実施形態で説明した利用履歴データ１０８と同様に、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。利用履歴データ３０８には、例えば、図４１に示すように、セキュアコンテナ３０４に格納されたコンテンツデータＣの識別子Ｃｏｎｔｅｎｔ＿ＩＤ、セキュアコンテナ３０４に格納されたコンテンツデータＣを提供したコンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、セキュアコンテナ３０４を配給したサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータＣの信号諸元データ、セキュアコンテナ３０４内のコンテンツデータＣの圧縮方法、セキュアコンテナ３０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ３０４を配給を受けたＳＡＭ３０$5_1$～３０$5_4$の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭ１０$5_1$～１０$5_4$のユーザのＵＳＥＲ＿ＩＤなどが記述されている。従って、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク３０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【０２４６】証明書・権利書管理部４４５は、ＣＥＲデータベース４４５ａに登録されて権威化された公開鍵証明書データCER_{cp}、公開鍵証明書データCER_{SP}および公開鍵証明書データCER_{SAM1}～CER_{SAM2}などを読み出すと共に、コンテンツプロバイダ３０１の権利書データ１０６およびコンテンツ鍵データＫｃ、並びにサービスプロバイダ３１０のプライスタグデータ３１２などをＣＥＲデータベース４４５ａに登録して権威化する。このとき、証明書・権利書管理部４４５は、権利書データ１０６、コンテンツ鍵データＫｃおよびプライスタグデータ３１２などのハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いた署名データを付して権威化証明書データを作成する。

90

【０２４７】コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１との間で通信する機能を有し、登録されているコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤなどを管理するＣＰデータベース１４８ａにアクセスできる。

【０２４８】ユーザ嗜好フィルタ生成部９０１は、利用履歴データ３０８に基づいて、当該利用履歴データ３０８を送信したＳＡＭ３０$5_1$～３０$5_4$のユーザの嗜好に応じたコンテンツデータＣを選択するためのユーザ嗜好フィルタデータ９０３を生成し、ユーザ嗜好フィルタデータ９０３をＳＡＭ管理部１４９を介して、当該利用履歴データ３０８を送信したＳＡＭ３０$5_1$～３０$5_4$に送信する。

【０２４９】マーケティング情報データ生成部９０２は、利用履歴データ３０８に基づいて、例えば、複数のサービスプロバイダ３１０によってユーザホームネットワーク１０３に配給されたコンテンツデータＣの全体の購入状況などを示すマーケティング情報データ９０４を生成し、これをサービスプロバイダ管理部３９０を介して、サービスプロバイダ３１０に送信する。サービスプロバイダ３１０は、マーケティング情報データ９０４を参考にして、今後提供するサービスの内容を決定する。

【０２５０】以下、ＥＭＤサービスセンタ３０２内での処理の流れを説明する。ＥＭＤサービスセンタ３０２からコンテンツプロバイダ３０１への配信用鍵データKD_1～KD_6の送信と、ＥＭＤサービスセンタ３０２からＳＡＭ３０$5_1$～３０$5_4$への配信用鍵データKD_1～KD_3の送信とは、第１実施形態の場合と同様に行なわれる。

【０２５１】また、ＥＭＤサービスセンタ３０２がコンテンツプロバイダ３０１から、公開鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部４４５がＣＥＲデータベース４４５ａに対して登録を行なう点を除いて、前述した第１実施形態の場合と同様に行なわれる。

【０２５２】次に、ＥＭＤサービスセンタ３０２がサービスプロバイダ３１０から、公開鍵証明書データの発行要求を受けた場合の処理を、図３８を参照しながら説明する。この場合に、サービスプロバイダ管理部３９０は、予めＥＭＤサービスセンタ３０２によって与えられたサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、公開鍵データ$K_{SP,P}$および署名データ$SIG_{70,SP}$をサービスプロバイダ３１０から受信すると、これらを、相互認証部１５０と図３４に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データ$SIG_{70,SP}$の

正当性を署名処理部４４３において確認した後に、識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ３１０がＳＰデータベース３９０ａに登録されているか否かを確認する。そして、証明書・権利書管理部４４５は、当該サービスプロバイダ３１０の公開鍵証明書データＣＥＲ$_{SP}$をＣＥＲデータベース４４５ａから読み出してサービスプロバイダ管理部３９０に出力する。また、署名処理部４４３は、公開鍵証明書データＣＥＲ$_{SP}$のハッシュ値をとり、ＥＭＤサービスセンタ３０２の秘密鍵データ$K_{ESC,S}$を用いて、署名データＳＩＧ$_{61,ESC}$を作成し、これをサービスプロバイダ管理部３９０に出力する。そして、サービスプロバイダ管理部３９０は、公開鍵証明書データＣＥＲ$_{SP}$およびその署名データＳＩＧ$_{61,ESC}$を、相互認証部１５０と図３４に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ３１０に送信する。

【０２５３】なお、ＥＭＤサービスセンタ３０２がＳＡＭ１０５$_1$～１０５$_4$から、公開鍵証明書データの発行要求を受けた場合の処理は、第１実施形態と同様である。また、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１から権利書データ１０６の登録要求を受けた場合の処理も、第１実施形態と同様である。

【０２５４】次に、ＥＭＤサービスセンタ３０２が、サービスプロバイダ３１０からプライスタグデータ３１２の登録要求を受けた場合の処理を、図３８を参照しながら説明する。この場合には、サービスプロバイダ管理部３９０がサービスプロバイダ３１０から図３７に示すプライスタグ登録要求モジュールＭｏｄ$_{102}$を受信すると、相互認証部１５０と図３４に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いてプライスタグ登録要求モジュールＭｏｄ$_{102}$を復号する。そして、当該復号したプライスタグ登録要求モジュールＭｏｄ$_{102}$に格納された署名データＳＩＧ$_{80,SP}$の正当性を署名処理部４４３において確認した後に、プライスタグ登録要求モジュールＭｏｄ$_{102}$に格納されたプライスタグデータ３１２を、証明書・権利書管理部４４５を介してＣＥＲデータベース４４５ａに登録して権威化する。

【０２５５】次に、ＥＭＤサービスセンタ３０２において決済を行なう場合の処理を図４０を参照しながら説明する。ＳＡＭ管理部１４９は、ユーザホームネットワーク３０３の例えばＳＡＭ３０５$_1$から利用履歴データ３０８およびその署名データＳＩＧ$_{205,SAM1}$を入力すると、利用履歴データ３０８および署名データＳＩＧ$_{205,SAM1}$を、相互認証部１５０とＳＡＭ３０５$_1$～３０５$_4$との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、ＳＡＭ３０５$_1$の公開鍵データ$K_{SAM1,P}$を用いて署名データＳＩＧ$_{205,SAM1}$の検証

を行なった後に、決算処理部４４２に出力する。

【０２５６】そして、決済処理部４４２は、ＳＡＭ３０５$_1$から入力した利用履歴データ３０８と、証明書・権利書管理部４４５から入力した標準小売価格データＳＲＰおよびプライスタグデータ３１２とに基づいて決済処理を行う。決済処理部４４２は、決済処理により、図４０に示すように、コンテンツプロバイダ３０１についての決済レポートデータ３０７ｃおよび決済請求権データ１５２ｃを作成し、これらをそれぞれコンテンツプロバイダ管理部１４８および決算機関管理部１４４に出力する。また、決済処理により、図３８および図４０に示すように、サービスプロバイダ３１０についての決済レポートデータ３０７ｓおよび決済請求権データ１５２ｓを作成し、これらをそれぞれサービスプロバイダ管理部３９０および決算機関管理部１４４に出力する。

【０２５７】次に、決算機関管理部１４４は、決済請求権データ１５２ｃ，１５２ｓと、それらについて秘密鍵データ$K_{ESC,S}$を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図３２に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。これにより、決済請求権データ１５２ｃに示される金額の金銭がコンテンツプロバイダ３０１に支払われ、決済請求権データ１５２ｓに示される金額の金銭がサービスプロバイダ３１０に支払われる。

【０２５８】次に、ＥＭＤサービスセンタ３０２がコンテンツプロバイダ３０１およびサービスプロバイダ３１０に決済レポートデータ３０７ｃおよび３０７ｓを送信する場合の処理を説明する。決算処理部４４２において決済が行なわれると、決算処理部４４２からコンテンツプロバイダ管理部１４８に決済レポートデータ３０７ｃが出力される。コンテンツプロバイダ管理部１４８は、決算処理部４４２から決済レポートデータ３０７ｃを入力すると、これを、相互認証部１５０と図３３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ３０１に送信する。また、決算処理部４４２において決済が行なわれると、決算処理部４４２からサービスプロバイダ管理部３９０に決済レポートデータ３０７ｓが出力される。サービスプロバイダ管理部３９０は、決算処理部４４２から決済レポートデータ３０７ｓを入力すると、これを、相互認証部１５０と図３４に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ３１０に送信する。

【０２５９】ＥＭＤサービスセンタ３０２は、その他に、第１実施形態のＥＭＤサービスセンタ１０２と同様に、ＳＡＭ３０５$_1$～３０５$_4$の出荷時の処理と、ＳＡＭ登録リストの登録処理とを行なう。

【０２６０】〔ユーザホームネットワーク３０３〕ユー

ザホームネットワーク３０３は、図３２に示すように、ネットワーク機器３６０$_1$およびＡ／Ｖ機器３６０$_2$～３６０$_4$を有している。ネットワーク機器３６０$_1$は、ＣＡモジュール３１１およびＳＡＭ３０５$_1$を内蔵している。また、ＡＶ機器３６０$_2$～３６０$_4$は、それぞれＳＡＭ３０５$_2$～３０５$_4$を内蔵している。ＳＡＭ３０５$_1$～３０５$_4$の相互間は、例えば、１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。なお、ＡＶ機器３６０$_2$～３６０$_4$は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器３６０$_1$のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク３０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０２６１】以下、ネットワーク機器３６０$_1$について説明する。図４２は、ネットワーク機器３６０$_1$の構成図である。図４２に示すように、ネットワーク機器３６０$_1$は、通信モジュール１６２、ＣＡモジュール３１１、復号モジュール９０５、ＳＡＭ３０５$_1$、復号・伸長モジュール１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。図４２において、図８と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。

【０２６２】通信モジュール１６２は、サービスプロバイダ３１０との間の通信処理を行なう。具体的には、通信モジュール１６２は、サービスプロバイダ３１０から衛星放送などで受信したセキュアコンテナ３０４を復号モジュール９０５に出力する。また、通信モジュール１６２は、サービスプロバイダ３１０に電話回線などを介してＳＰ用購入履歴データ３０９を受信したユーザ嗜好フィルタデータ９００をＣＡモジュール３１１に出力すると共に、ＣＡモジュール３１１から入力したＳＰ用購入履歴データ３０９を電話回線などを介してサービスプロバイダ３１０に送信する。

【０２６３】図４３は、ＣＡモジュール３１１および復号モジュール９０５の機能ブロック図である。図４３に示すように、ＣＡモジュール３１１は、相互認証部９０６、記憶部９０７、暗号化・復号部９０８およびＳＰ用購入履歴データ生成部９０９を有する。相互認証部９０６は、ＣＡモジュール３１１とサービスプロバイダ３１０との間で電話回線を介してデータを送受信する際に、サービスプロバイダ３１０との間で相互認証を行ってセッション鍵データK_{SES}を生成し、これを暗号化・復号部９０８に出力する。

【０２６４】記憶部９０７は、例えば、サービスプロバイダ３１０とユーザとの間で契約が成立した後に、サービスプロバイダ３１０からＩＣカード９１２などを用いてオフラインで供給されたマスタ鍵データK_Mを記憶する。

【０２６５】暗号化・復号部９０８は、復号モジュール９０５の復号部９１０からそれぞれ暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力し、記憶部９０７から読み出したマスタ鍵データK_Mを用いてワーク鍵データK_Wを復号する。そして、暗号化・復号部９０８は、当該復号したワーク鍵データK_Wを用いてスクランブル鍵データK_{SCR}を復号し、当該復号したスクランブル鍵データK_{SCR}を復号部９１０に出力する。また、暗号化・復号部９０８は、電話回線などを介して通信モジュール１６２がサービスプロバイダ３１０から受信したユーザ嗜好フィルタデータ９００を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して復号モジュール９０５のセキュアコンテナ選択部９１１に出力する。また、暗号化・復号部９０８は、ＳＰ用購入履歴データ生成部９０９から入力したＳＰ用購入履歴データ３０９を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して通信モジュール１６２を介してサービスプロバイダ３１０に送信する。

【０２６６】ＳＰ用購入履歴データ生成部９０９は、図４２に示す購入・利用形態決定操作部１６５を用いてユーザによるコンテンツデータＣの購入操作に応じた操作信号Ｓ１６５、またはＳＡＭ３０５$_1$からの利用制御状態データ１６６に基づいて、サービスプロバイダ３１０に固有のコンテンツデータＣの購入履歴を示すＳＰ用購入履歴データ３０９を生成し、これを暗号化・復号部９０８に出力する。ＳＰ用購入履歴データ３０９は、例えば、サービスプロバイダ３１０が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【０２６７】なお、ＣＡモジュール３１１は、サービスプロバイダ３１０が課金機能を有している場合には、サービスプロバイダ３１０の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、ＣＡモジュール３１１は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ３１０に送信する。

【０２６８】復号モジュール９０５は、復号部９１０およびセキュアコンテナ選択部９１１を有する。復号部９１０は、通信モジュール１６２から、それぞれ暗号化されたセキュアコンテナ３０４、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力する。そして、復号部９１０は、暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_WをＣＡモジュール３１１の暗号化・復号部９０８に出力し、暗号化・復号部９０８から復号されたスクランブル鍵データK_{SCR}を入力する。そして、復号部９１０は、暗号化されたセキュアコンテナ３０４を、スクランブル鍵データK_{SCR}を用いて

復号した後に、セキュアコンテナ選択部９１１に出力する。

【０２６９】なお、セキュアコンテナ３０４が、MPEG2 Transport Stream 方式でサービスプロバイダ３１０から送信される場合には、例えば、復号部９１０は、TS Packet 内のＥＣＭ(Entitlement Control Message) からスクランブル鍵データK_{SCR}を取り出し、ＥＭＭ(Entitlement Management Message)からワーク鍵データＫｗを取り出す。ＥＣＭには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、ＥＭＭは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【０２７０】セキュアコンテナ選択部９１１は、復号部９１０から入力したセキュアコンテナ３０４を、ＣＡモジュール３１１から入力したユーザ嗜好フィルタデータ９００を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ３０４を選択してＳＡＭ３０$5_1$ に出力する。

【０２７１】次に、ＳＡＭ３０$5_1$について説明する。なお、ＳＡＭ３０$5_1$は、サービスプロバイダ３１０についての署名検証処理を行なうなど、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０に関しての処理を行う点を除いて、図１０～図２４を用いて前述した第１実施形態のＳＡＭ１０$5_1$と基本的に行なう機能および構造を有している。また、ＳＡＭ３０$5_2$～３０$5_4$は、ＳＡＭ３０$5_1$と基本的に同じ機能を有している。すなわち、ＳＡＭ３０$5_1$～３０$5_4$は、コンテンツ単位の課金処理をおこなうモジュールであり、ＥＭＤサービスセンタ３０２との間で通信を行う。

【０２７２】以下、ＳＡＭ３０$5_1$の機能について詳細に説明する。図４４は、ＳＡＭ３０$5_1$の機能の構成図である。なお、図４４には、サービスプロバイダ３１０からセキュアコンテナ３０４を入力し、セキュアコンテナ３０４内のキーファイルＫＦを復号する処理に関連するデータの流れが示されている。図４４に示すように、ＳＡＭ３０$5_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、誤り訂正部１８１、ダウンロードメモリ管理部１８２、セキュアコンテナ復号部１８３、復号・伸長モジュール管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、署名処理部１８９、ＳＡＭ管理部１９０、記憶部１９２、メディアＳＡＭ管理部１９７、スタックメモリ２００、サービスプロバイダ管理部５８０、課金処理部５８７、署名処理部５９８および外部メモリ管理部８１１を有する。なお、図４４に示すＳＡＭ３０$5_1$の所定の機能は、ＳＡＭ１０$5_1$の場合と同様に、ＣＰＵにおいて秘密プログラムを実行することによって実現される。図４４において、図１０と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと同じである。

【０２７３】また、図４２に示す外部メモリ２０１には、第１実施形態で説明した処理および後述する処理を経て、利用履歴データ３０８およびＳＡＭ登録リストが記憶される。また、スタックメモリ２００には、図４５に示すように、コンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOC}、コンテンツプロバイダ３０１の公開鍵証明書データCER_{CP}、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}、利用制御状態データ（ＵＣＳ）３６６、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3およびプライスタグデータ３１２などが記憶される。

【０２７４】以下、ＳＡＭ３０$5_1$の機能ブロックのうち、図４４において新たに符号を付した機能ブロックについて説明する。署名処理部５８９は、記憶部１９２あるいはスタックメモリ２００から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$、コンテンツプロバイダ３０１の公開鍵データ$K_{cp,p}$およびサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$を用いて、セキュアコンテナ３０４内の署名データの検証を行なう。

【０２７５】課金処理部５８７は、図４６に示すように、図４２に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５と、スタックメモリ２００から読み出されたプライスタグデータ３１２とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。課金処理部５８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御状態データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【０２７６】また、課金処理部５８７は、課金処理において、利用履歴データ３０８を生成し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。ここで、利用履歴データ３０８は、第１実施形態の利用履歴データ１０８と同様に、ＥＭＤサービスセンタ３０２において、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。

【０２７７】また、課金処理部５８７は、操作信号Ｓ１６５に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態（UCS: Usage Control Status)データ１６６を生成し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられ

97

る。利用制御状態データ１６６には、コンテンツのＩＤ、購入形態、買い切り価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０２７８】なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ３０５$_1$からサービスプロバイダ３１０に利用制御状態データ１６６をリアルタイムに送信し、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２に、利用履歴データ１０８をＳＡＭ１０５$_1$に取りにいくことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ１６６が、サービスプロバイダ３１０およびＥＭＤサービスセンタ３０２にリアルタイムに送信される。

【０２７９】また、ＳＡＭ３０５$_1$では、ＥＭＤサービスセンタ管理部１８５がＥＭＤサービスセンタ３０２から受信したユーザ嗜好フィルタデータ９０３が、サービスプロバイダ管理部５８０に出力される。そして、サービスプロバイダ管理部５８０において、図４２に示す復号モジュール９０５から入力したセキュアコンテナ３０４が、ユーザ嗜好フィルタデータ９０３に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ３０４が選択され、当該選択されたセキュアコンテナ３０４が誤り訂正部１８１に出力される。これにより、ＳＡＭ３０５$_1$において、当該ＳＡＭ３０５$_1$のユーザが契約している全てのサービスプロバイダ３１０を対象として、当該ユーザによるコンテンツデータＣの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータＣの選択処理が可能になる。

【０２８０】以下、ＳＡＭ３０５$_1$内での処理の流れを説明する。ＥＭＤサービスセンタ３０２から受信した配信用鍵データKD_1～KD_3を記憶部１９２に格納する際のＳＡＭ３０５$_1$内での処理の流れは、前述したＳＡＭ１０５$_1$の場合と同様である。

【０２８１】次に、セキュアコンテナ３０４をサービスプロバイダ３１０から入力し、セキュアコンテナ３０４内のキーファイルＫＦを復号する際のＳＡＭ３０５$_1$内での処理の流れを図４４を参照しながら説明する。相互認証部１７０と図３４に示すサービスプロバイダ３１０の相互認証部３５２との間で相互認証が行なわれる。暗号化・復号部１７１は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、サービスプロバイダ管理部５８０を介してサービスプロバイダ３１０から受信した図３５に示すセキュアコンテナ３０４を復号する。

【０２８２】次に、署名処理部５８９は、図３５（Ｄ）に示す署名データ$SIG_{61,ESC}$の検証を行なった後に、図３５（Ｄ）に示す公開鍵証明書データ$CERT_{SP}$内に格納されたサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$の正当性を確認する。サービスプロバイダ管理部５８０は、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$の正当性が確認されると、セキュアコンテナ３０４を誤り訂正部１８１に出力する。

98

【０２８３】誤り訂正部１８１は、セキュアコンテナ３０４を誤り訂正した後に、ダウンロードメモリ管理部１８２に出力する。ダウンロードメモリ管理部１８２は、相互認証部１７０と図４２に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ３０４をダウンロードメモリ１６７に書き込む。

【０２８４】次に、ダウンロードメモリ管理部１８２は、相互認証部１７０と図４２に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ３０４に格納された図３５（Ｂ）に示すキーファイルＫＦを読み出してセキュアコンテナ復号部１８３に出力する。

【０２８５】そして、セキュアコンテナ復号部１８３は、記憶部１９２から入力した対応する期間の配信用鍵データKD_1～KD_3を用いて、キーファイルＫＦを復号し、図３５（Ｂ）に示す署名・証明書モジュールMod_1に格納された署名データ$SIG_{1,ESC}$、$SIG_{2,cp}$～$SIG_{4,cp}$を署名処理部５８９に出力する。署名処理部５８９は、図３５（Ｂ）に示す署名データ$SIG_{1,ESC}$の検証を行なった後に、公開鍵証明書データ$CERT_{cp}$内に格納された公開鍵データ$K_{CP,P}$を用いて署名データ$SIG_{2,cp}$～$SIG_{4,cp}$の検証を行なう。

【０２８６】次に、セキュアコンテナ復号部１８３は、署名データ$SIG_{2,cp}$～$SIG_{4,cp}$の正当性が確認されると、キーファイルＫＦをスタックメモリ２００に書き込む。

【０２８７】以下、サービスプロバイダ３１０からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ３０４の購入形態を決定するまでの処理の流れを図４６を参照しながら説明する。ユーザによる図４２に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が課金処理部５８７に出力されると、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、復号・伸長モジュール管理部１８４を介して、図４２に示す復号・伸長モジュール１６３に出力される。このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。コンテンツファイルＣＦは、図４２に示す復号部２２１において復号された後に、復号部２２２に出力される。

【０２８８】また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデ

ータ１９９が、図４２に示す復号・伸長モジュール１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。次に、電子透かし情報処理部２２４においてユーザ電子透かし情報用データ１９６がコンテンツデータＣに埋め込まれた後、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される

【０２８９】そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。そして、課金処理部１８７において、決定された購入形態に応じた利用履歴データ３０８および利用制御状態データ１６６が生成され、利用履歴データ３０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に利用制御状態データ１６６がスタックメモリ２００に書き込まれる。以後は、利用監視部１８６において、利用制御状態データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。そして、スタックメモリ２００に格納されているキーファイルＫＦに、利用制御状態データ１６６が加えられ、購入形態が決定した後述する図４７に示す新たなキーファイルKF_{11}が生成される。キーファイルKF_{11}は、スタックメモリ２００に記憶される。図４７に示すように、キーファイルKF_1に格納された利用制御状態データ１６６はストレージ鍵データK_{STR}を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{300}が付されている。また、利用制御状態データ１６６およびMAC_{300}からなるモジュールは、メディア鍵データ$_{MED}$を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データK_{MED}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{301}が付されている。

【０２９０】次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図４６を参照しながら説明する。この場合には、利用監視部１８６の監視下で、操作信号Ｓ１６５に基づいて、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、図４２に示す復号・伸長モジュール１６３に出力される。また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃが復号・伸長モジュール１６３に出力される。そして、復号・伸長モジュール１６３の復号部２２２において、コンテンツ鍵データＫｃを用いたコンテンツファイルＣＦの復号と、伸長部２２３による伸長処理とが行なわれ、再生モジュール１６９において、コンテンツデータＣが再生される。このとき、課金処理部５８７において、操作信号Ｓ１６５に応じて、利用履歴データ３０８が更新される。利用履歴データ３０８は、秘密鍵データ$K_{SAM1,S}$を用いて作成したそれぞれ署名データ$SIG_{205,SAM1}$と共に、ＥＭＤサービスセンタ管理部１８５を介して、所定のタイミングで、ＥＭＤサービスセンタ３０２に送信される。

【０２９１】次に、図４８に示すように、例えば、ネットワーク機器360_1のダウンロードメモリ１６７にダウンロードされた既に購入形態が決定されたコンテンツファイルＣＦを、バス１９１を介して、ＡＶ機器360_2のＳＡＭ305_2に転送する場合のＳＡＭ305_1内での処理の流れを図４９を参照しながら説明する。ユーザは、購入・利用形態決定操作部１６５を操作して、ダウンロードメモリ１６７に記憶された所定のコンテンツをＡＶ機器360_2に転送することを指示し、当該操作に応じた操作信号Ｓ１６５が、課金処理部５８７に出力される。これにより、課金処理部５８７は、操作信号Ｓ１６５に基づいて、スタックメモリ２００に記憶されている利用履歴データ３０８を更新する。

【０２９２】また、ダウンロードメモリ管理部１８２は、ダウンロードメモリ１６７から読み出した図５０（Ａ）に示すコンテンツファイルＣＦをＳＡＭ管理部１９０に出力する。また、スタックメモリ２００から読み出した図５０（Ｂ）に示す既に購入形態が決定されたキーファイルKF_{11}を、署名処理部５８９およびＳＡＭ管理部１９０に出力する。署名処理部５８９は、キーファイルKF_{11}の署名データ$SIG_{80,SAM1}$を作成し、これをＳＡＭ管理部１９０に出力する。また、ＳＡＭ管理部１９０は、記憶部１９２から、図５０（Ｃ）に示す公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$を読み出す。

【０２９３】また、相互認証部１７０は、ＳＡＭ305_2との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部１７１に出力する。ＳＡＭ管理部１９０は、図５０（Ａ），（Ｂ），（Ｃ）に示すデータを、暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて暗号化した後に、図４９に示すＡＶ機器360_2のＳＡＭ305_2に出力する。

【０２９４】以下、図４８に示すように、ＳＡＭ305_1から入力したコンテンツファイルＣＦなどを、ＲＡＭ型などの記録媒体（メディア）に書き込む際のＳＡＭ305_2内での処理の流れを、図５１を参照しながら説明

101

する。

【０２９５】この場合には、ＳＡＭ３０５$_2$のＳＡＭ管理部１９０は、図５１に示すように、図５０（Ａ）に示すコンテンツファイルＣＦ、図５０（Ｂ）に示すキーファイルＫＦ$_{11}$およびその署名データＳＩＧ$_{80,SAM1}$と、図５０（Ｃ）に示す公開鍵署名データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22,ESC}$とを、ネットワーク機器３６０$_1$のＳＡＭ３０５$_1$から入力する。そして、暗号化・復号部１７１において、ＳＡＭ管理部１９０が入力したコンテンツファイルＣＦと、キーファイルＫＦ$_{11}$およびその署名データＳＩＧ$_{80,SAM1}$と、公開鍵署名データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22,ESC}$とが、相互認証部１７０とＳＡＭ３０５$_1$の相互認証部１７０との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて復号される。

【０２９６】次に、セッション鍵データＫ$_{SES}$を用いて復号されたコンテンツファイルＣＦがメディアＳＡＭ管理部１９７に出力される。また、セッション鍵データＫ$_{SES}$を用いて復号されたキーファイルＫＦ$_{11}$およびその署名データＳＩＧ$_{80,SAM1}$と、公開鍵署名データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22,ESC}$とが、スタックメモリ２００に書き込まれる。

【０２９７】次に、署名処理部５８９は、スタックメモリ２００から読み出した署名データＳＩＧ$_{22,ESC}$を、記憶部１９２から読み出した公開鍵データＫ$_{ESC,P}$を用いて検証して、公開鍵証明書データＣＥＲ$_{SAM1}$の正当性を確認する。そして、署名処理部５８９は、公開鍵証明書データＣＥＲ$_{SAM1}$の正当性を確認すると、公開鍵証明書データＣＥＲ$_{SAM1}$に格納された公開鍵データＫ$_{SAM1,P}$を用いて、署名データＳＩＧ$_{80,SAM1}$の正当を確認する。

【０２９８】次に、署名データＳＩＧ$_{80,SAM1}$の正当を確認されると、図５０（Ｂ）に示すキーファイルＫＦ$_{11}$をスタックメモリ２００から読み出して暗号化・復号部１７３に出力する。そして、暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データＫ$_{STR}$、メディア鍵データＫ$_{MED}$および購入者鍵データＫ$_{PIN}$を用いてキーファイルＫＦ$_{11}$を順に暗号化してメディアＳＡＭ管理部１９７に出力する。

【０２９９】メディアＳＡＭ管理部１９７は、ＳＡＭ管理部１９０から入力したコンテンツファイルＣＦおよび暗号化・復号部１７３から入力したキーファイルＫＦ$_{11}$を、図４８に示す記録モジュール２６０に出力する。そして、記録モジュール２６０は、メディアＳＡＭ管理部１９７から入力したコンテンツファイルＣＦおよびキーファイルＫＦ$_{11}$を、図４８に示すＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１に書き込む。

【０３００】なお、ＳＡＭ３０５$_1$内での処理のうち、コンテンツの購入形態が未決定のＲＯＭ型の記録媒体の購入形態を決定する際のＡＶ機器３６０$_2$内での処理の流れ、ＡＶ機器３６０$_3$において購入形態が未決定のＲ

102

ＯＭ型の記録媒体からセキュアコンテナ３０４を読み出してこれをＡＶ機器３６０$_2$に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ３１０の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ３１２を格納する点を除いて、第１実施形態のＳＡＭ１０５$_1$の場合と同じである。

【０３０１】次に、図３２に示すＥＭＤシステム３００の全体動作について説明する。図５２および図５３は、ＥＭＤシステム３００の全体動作のフローチャートである。ここでは、サービスプロバイダ３１０からユーザホームネットワーク３０３にオンラインでセキュアコンテナ３０４を送信する場合を例示して説明する。なお、以下に示す処理の前提として、ＥＭＤサービスセンタ３０２へのコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$の登録は既に終了しているものとする。

【０３０２】ステップＳ２１：ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データＫ$_{CP,P}$の公開鍵証明書ＣＥＲ$_{CP}$を、自らの署名データＳＩＧ$_{1,ESC}$と共にコンテンツプロバイダ３０１に送信する。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データＫ$_{SP,P}$の公開鍵証明書ＣＥＲ$_{SP}$を、自らの署名データＳＩＧ$_{61,ESC}$と共にサービスプロバイダ３１０に送信する。また、ＥＭＤサービスセンタ３０２は、各々有効期限が１カ月の６カ月分の配信用鍵データＫＤ$_1$～ＫＤ$_6$をコンテンツプロバイダ３０１に送信し、３カ月分の配信用鍵データＫＤ$_1$～ＫＤ$_3$をユーザホームネットワーク３０３のＳＡＭ３０５$_1$～３０５$_4$に送信する。

【０３０３】ステップＳ２２：コンテンツプロバイダ３０１は、図６（Ａ）に示す権利登録要求モジュールＭｏｄ$_2$を、ＥＭＤサービスセンタ３０２に送信する。そして、ＥＭＤサービスセンタ３０２は、所定の署名検証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化（認証）する。

【０３０４】ステップＳ２３：コンテンツプロバイダ３０１は、署名データの作成処理や、ＳＩＧ対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$などを用いた暗号化処理を経て、図４（Ａ），（Ｂ），（Ｃ）に示すデータを格納したセキュアコンテナ１０４を、サービスプロバイダ３１０に供給する。

【０３０５】ステップＳ２４：サービスプロバイダ３１０は、図４（Ｃ）に示す署名データＳＩＧ$_{1,ESC}$を検証した後に、公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{CP,P}$を用いて、図４（Ａ），（Ｂ）に示す署名データＳＩＧ$_{6,CP}$およびＳＩＧ$_{7,CP}$を検証して、セキュアコンテナ１０４が正当なコンテンツプロバイダ３０１から送信されたものであるかを確認する。

【０３０６】ステップＳ２５：サービスプロバイダ３１

０は、プライスタグデータ３１２を作成し、プライスタグデータ３１２を格納した図３５に示すセキュアコンテナ３０４を作成する。

【０３０７】ステップＳ２６：サービスプロバイダ３１０は、図３７に示すプライスタグ登録要求モジュールMod$_{102}$を、ＥＭＤサービスセンタ３０２に送信する。そして、ＥＭＤサービスセンタ３０２は、所定の署名検証を行った後に、プライスタグデータ３１２を登録して権威化する。

【０３０８】ステップＳ２７：サービスプロバイダ３１０は、例えば、ユーザホームネットワーク３０３のＣＡモジュール３１１からの要求に応じて、ステップＳ２５で作成したセキュアコンテナ３０４を、オンラインあるいはオフラインで、図４２に示すネットワーク機器３６０$_1$の復号モジュール９０５に送信する。

【０３０９】ステップＳ２８：ＣＡモジュール３１１は、ＳＰ用購入履歴データ３０９を作成し、これを所定のタイミングで、サービスプロバイダ３１０に送信する。

【０３１０】ステップＳ２９：SAM３０５$_1$～３０５$_4$のいずれかにおいて、図３５（Ｄ）に示す署名データ$SIG_{61,ESC}$を検証した後に、公開鍵証明書データCER_{SP}に格納された公開鍵データ$K_{SP,P}$を用いて、図３５（Ａ），（Ｂ），（Ｃ）に示す署名データ$SIG_{62,SP}$、$SIG_{63,SP}$，$SIG_{64,SP}$を検証して、セキュアコンテナ３０４が正当なサービスプロバイダ３１０から送信されたものであるかを確認する。

【０３１１】ステップＳ３０：SAM３０５$_1$～３０５$_4$のいずれかにおいて、配信用鍵データKD_1～KD_3を用いて、図３５（Ｂ）に示すキーファイルＫＦを復号する。そして、SAM３０５$_1$～３０５$_4$のいずれかにおいて、図３５（Ｂ）に示す署名データ$SIG_{1,ESC}$を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データ$K_{CP,P}$を用いて、図３５（Ｂ）に示す署名データ$SIG_{2,CP}$，$SIG_{3,CP}$および$SIG_{4,CP}$を検証して、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６が正当なコンテンツプロバイダ３０１によって作成されたものであるかを確認する。

【０３１２】ステップＳ３１：ユーザが図４２の購入・利用形態決定操作部１６５を操作してコンテンツの購入・利用形態を決定する。

【０３１３】ステップＳ３２：ステップＳ３１において生成された操作信号Ｓ１６５に基づいて、SAM３０５$_1$～３０５$_4$において、セキュアコンテナ３０４の利用履歴(Usage Log)データ３０８が生成される。SAM３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８およびその署名データ$SIG_{205,SAM1}$が送信される。

【０３１４】ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、決済請求権データ１５２ｃ，１５２ｓを作成する。

【０３１５】ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓを自らの署名データと共に送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者に分配される。

【０３１６】以上説明したように、ＥＭＤシステム３００によれば、ＥＭＤサービスセンタ３０２が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ３０１およびＥＭＤサービスセンタ３０２の所有者に、予め決められた比率に従って確実に分配される。また、ＥＭＤシステム３００によれば、同じコンテンツプロバイダ３０１が供給した同じコンテンツファイルＣＦについての権利書データ１０６は、サービスプロバイダ３１０のサービス形態とは無関係に、そのままSAM３０５$_1$～３０５$_4$に供給される。従って、SAM３０５$_1$～３０５$_4$において、権利書データ１０６に基づいて、コンテンツプロバイダ３０１の意向通りに、コンテンツファイルＣＦの利用を行わせることができる。すなわち、ＥＭＤシステム３００によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織７２５に頼ることなく、技術的な手段によって、コンテンツプロバイダ３０１の所有者の権利および利益を確実に守ることができる。

【０３１７】第２実施形態の第１変形例

図５４は、第２実施形態の第１変形例に係わる２個のサービスプロバイダを用いたＥＭＤシステム３００ａの構成図である。図５４において、図３２と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。図５４に示すように、ＥＭＤシステム３００ａでは、コンテンツプロバイダ３０１からサービスプロバイダ３１０ａおよび３１０ｂに、同じセキュアコンテナ１０４を供給する。

【０３１８】サービスプロバイダ３１０ａは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータＣと、当該コンテンツデータＣについて独自に作成したプライスタグデータ３１２ａとを格納したセキュアコンテナ３０４ａを作成し、これをネットワーク機器３６０$_1$に配給する。また、サービスプロバイダ３１０ｂは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータＣと、当該コンテンツデータＣについて独自に作成したプライスタグデータ３１２ｂと

105

を格納したセキュアコンテナ３０４ｂを作成し、これをネットワーク機器360_1に配給する。ここで、セキュアコンテナ３０４ａ，３０４ｂのフォーマットは、図３５を用いた説明したセキュアコンテナ３０４と同じである。

【０３１９】ネットワーク機器$360a_1$には、サービスプロバイダ３１０ａ，３１０ｂの各々に対応したＣＡモジュール３１１ａ，３１１ｂが設けられている。ＣＡモジュール３１１ａ，３１１ｂは、自らの要求に応じたセキュアコンテナ３０４ａ，３０４ｂの配給を、それぞれサービスプロバイダ３１０ａ，３１０ｂから受ける。

【０３２０】次に、ＣＡモジュール３１１ａ，３１１ｂは、配給されたセキュアコンテナ３０４ａ，３０４ｂに応じたＳＰ用購入履歴データ３０９ａ，３０９ｂをそれぞれ作成し、これらをそれぞれサービスプロバイダ３１０ａ，３１０ｂに送信する。また、ＣＡモジュール３１１ａ，３１１ｂは、セキュアコンテナ３０４ａ，３０４ｂをセッション鍵データK_{SES}で復号した後に、ＳＡＭ305_1～305_4に出力する。

【０３２１】次に、ＳＡＭ305_1～305_4において、共通の配信用鍵データKD_1～KD_3を用いて、セキュアコンテナ３０４ａ，３０４ｂ内のキーファイルＫＦが復号され、共通の権利書データ１０６に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ３０８が作成される。

【０３２２】そして、ＳＡＭ305_1～305_4からＥＭＤサービスセンタ３０２に、利用履歴データ３０８が送信される。

【０３２３】ＥＭＤサービスセンタ３０２では、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０ａ，３１０ｂの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ１５２ｃ，１５２ｓａ，１５２ｓｂを作成する。

【０３２４】ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓａ，１５２ｓｂを送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０ａ，３１０ｂの所有者に分配される。

【０３２５】上述したように、ＥＭＤシステム３００ｂによれば、同じコンテンツファイルＣＦをサービスプロバイダに３１０ａ，３１０ｂに供給する場合に、当該コンテンツファイルＣＦについての権利書データ１０６を配信用鍵データKD_1～KD_6で暗号化してサービスプロバイダに３１０ａ，３１０ｂに供給し、サービスプロバイダに３１０ａ，３１０ｂは暗号化された権利書データ１０６をそのまま格納したセキュアコンテナ３０４

106

ａ，３０４ｂをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のＳＡＭ3051_1～3054_4では、コンテンツファイルＣＦをサービスプロバイダに３１０ａ，３１０ｂの何れから配給を受けた場合でも、共通の権利書データ１０６に基づいて権利処理を行うことができる。

【０３２６】なお、上述した第１変形例では、２個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【０３２７】第２実施形態の第２変形例

図５５は、第２実施形態の第２変形例に係わる複数のコンテンツプロバイダを用いたＥＭＤシステム３００ｂの構成図である。図５５において、図３２と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。図５５に示すように、ＥＭＤシステム３００ｂでは、コンテンツプロバイダ３０１ａ，３０１ｂからサービスプロバイダ３１０に、それぞれセキュアコンテナ１０４ａ，１０４ｂが供給される。

【０３２８】サービスプロバイダ３１０は、例えば、コンテンツプロバイダ３０１ａ，３０１ｂが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ１０４ａについてのプライスタグデータ３１２ａと、セキュアコンテナ１０４ｂについてのプライスタグデータ３１２ｂとをそれぞれ生成し、これらを格納したセキュアコンテナ３０４ｃを作成する。図５５に示すように、セキュアコンテナ３０４ｃには、コンテンツファイルＣＦａ，ＣＦｂ、キーファイルＫＦａ，ＫＦｂ、プライスタグデータ３１２ａ，３１２ｂ、それらの各々についてのサービスプロバイダ３１０の秘密鍵データ$K_{CP,S}$による署名データが格納されている。

【０３２９】セキュアコンテナ３０４ｃは、ユーザホームネットワーク３０３のネットワーク機器360_1のＣＡモジュール３１１で受信された後に、ＳＡＭ3051_1～3054_4において処理される。

【０３３０】ＳＡＭ3051_1～3054_4では、配信用鍵データKDa_1～KDa_3を用いて、キーファイルＫＦａが復号され、権利書データ１０６ａに基づいて、コンテンツファイルＣＦａについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ３０８に記述される。また、ＳＡＭ3051_1～3054_4において、配信用鍵データKDb_1～KDb_3を用いて、キーファイルＫＦｂが復号され、権利書データ１０６ｂに基づいて、コンテンツファイルＣＦｂについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ３０８に記述される。

【０３３１】そして、ＳＡＭ3051_1～3054_4からＥＭＤサービスセンタ３０２に、利用履歴データ３０８が送信される。

【０３３２】ＥＭＤサービスセンタ３０２では、利用履

歴データ３０８に基づいて、コンテンツプロバイダ３０１ａ，３０１ｂおよびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ１５２ｃａ，１５２ｃｂ，１５２ｓを作成する。

【０３３３】ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃａ，１５２ｃｂ，１５２ｓを送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１ａ，３０１ｂおよびサービスプロバイダ３１０の所有者に分配される。

【０３３４】上述したように、ＥＭＤシステム３００ｂによれば、セキュアコンテナ３０４ｃ内に格納されたコンテンツファイルＣＦａ，ＣＦｂの権利書データ１０６ａ，１０６ｂは、コンテンツプロバイダ３０１ａ，３０１ｂが作成したものをそのまま用いるため、ＳＡＭ３０５$_1$～３０５$_4$内において、権利書データ１０６ａ，１０６ｂに基づいて、コンテンツファイルＣＦａ，ＣＦｂについての権利処理がコンテンツプロバイダ３０１ａ，３０１ｂの意向に沿って確実に行われる。

【０３３５】なお、図５５に示す第２変形例では、２個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【０３３６】第２実施形態の第３変形例

図５６は、第２実施形態の第３変形例に係わるＥＭＤシステムの構成図である。上述した第２実施形態では、ＥＭＤサービスセンタ３０２が決済機関９１に対して、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済を行う場合を例示したが、本発明では、例えば、図５６に示すように、ＥＭＤサービスセンタ３０２において、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１のための決済請求権データ１５２ｃと、サービスプロバイダ３１０のための決済請求権データ１５２ｓとを作成し、これらをそれぞれコンテンツプロバイダ３０１およびサービスプロバイダ３１０に送信するようにしてもよい。この場合には、コンテンツプロバイダ３０１は、決済請求権データ１５２ｃを用いて、ペイメントゲートウェイ９０ａを介して決済機関９１ａに決済を行う。また、サービスプロバイダ３１０は、決済請求権データ１５２ｓを用いて、ペイメントゲートウェイ９０ｂを介して決済機関９１ｂに決済を行う。

【０３３７】第２実施形態の第４変形例

図５７は、第２実施形態の第４変形例に係わるＥＭＤシステムの構成図である。上述した第２実施形態では、例えば現行のインターネットのようにサービスプロバイダ３１０が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ３１０が課金機能を有している場合には、ＣＡモジュール３１１において、セキュアコンテナ３０４に関するサービスプロバイダ３１０のサービスに対しての利用履歴データ３０８ｓを作成してサービスプロバイダ３１０に送信する。そして、サービスプロバイダ３１０は、利用履歴データ３０８ｓに基づいて、課金処理を行って決済請求権データ１５２ｓを作成し、これを用いてペイメントゲートウェイ９０ｂを介して決済機関９１ｂに決済を行う。一方、ＳＡＭ３０５$_1$～３０５$_4$は、セキュアコンテナ３０４に関するコンテンツプロバイダ３０１の権利処理に対しての利用履歴データ３０８ｃを作成し、これをＥＭＤサービスセンタ３０２に送信する。ＥＭＤサービスセンタ３０２は、利用履歴データ３０８ｃに基づいて、決済請求権データ１５２ｃを作成し、これをコンテンツプロバイダ３０１に送信する。コンテンツプロバイダ３０１は、決済請求権データ１５２ｃを用いて、ペイメントゲートウェイ９０ａを介して決済機関９１ａに決済を行う。

【０３３８】第２実施形態の第５変形例

上述した実施形態では、図４０に示すように、ＥＭＤサービスセンタ３０２のユーザ嗜好フィルタ生成部９０１において、ＳＡＭ３０５$_1$などから受信した利用履歴データ３０８に基づいて、ユーザ嗜好フィルタデータ９０３を生成する場合を例示したが、例えば、図４６に示すＳＡＭ３０５$_1$などの利用監視部１８６で生成した利用制御状態データ１６６をリアルタイムでＥＭＤサービスセンタ３０２に送信するようにして、ＳＰ用購入履歴データ３０９において、利用制御状態データ１６６に基づいてユーザ嗜好フィルタデータ９０３を生成するようにしてもよい。

【０３３９】第２実施形態の第６変形例

コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$は、それぞれ自らの公開鍵データ$K_{CP,P}$，$K_{SP,P}$，$K_{SAM1,P}$～$K_{SAM4,P}$の他に、自らの秘密鍵データ$K_{CP,S}$，$K_{SP,S}$，$K_{SAM1,S}$～$K_{SAM4,S}$をＥＭＤサービスセンタ３０２に登録してもよい。このようにすることで、ＥＭＤサービスセンタ３０２は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データ$K_{CP,S}$，$K_{SP,S}$，$K_{SAM1,S}$～$K_{SAM4,S}$を用いて、コンテンツプロバイダ３０１とサービスプロバイダ３１０との間の通信、サービスプロバイダ３１０とＳＡＭ３０５$_1$～３０５$_4$との間の通信、並びにユーザホームネットワーク３０３内でのＳＡＭ３０５$_1$～３０５$_4$相互間での通信のうち対象となる通信を盗聴することが可能になる。また、ＳＡＭ３０５$_1$～３０５$_4$については、出荷時に、ＥＭＤサービスセンタ３０２によって秘密鍵データ$K_{SAM1,S}$～$K_{SAM4,S}$を生成し、これをＳＡＭ３０５$_1$～３０５$_4$に格納すると共にＥＭＤサービスセンタ３０２が保持（登録）するようにしてもよい。

109

【０３４０】第２実施形態の第７変形例

上述した実施形態では、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が、相互に通信を行う場合に、ＥＭＤサービスセンタ３０２から事前に公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$，ＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAN4}$を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。例えば、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が、相互に通信を行う場合に、ＥＭＤサービスセンタ３０２から事前に公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$，ＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAN4}$を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。また、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が、通信時に、ＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$，ＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAN4}$を取得してもよい。

【０３４１】図５８は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。なお、図５８において、図３２と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク３０３ａは、前述したユーザホームネットワーク３０３と同じである。ユーザホームネットワーク３０３ｂでは、ＩＥＥＥ１３９４シリアルバスであるバス１９１を介してＳＡＭ３０５$_{11}$～３０５$_{14}$を接続している。

【０３４２】コンテンツプロバイダ３０１がサービスプロバイダ３１０の公開鍵証明書データＣＥＲ$_{SP}$を取得する場合には、例えば、通信に先立ってサービスプロバイダ３１０からコンテンツプロバイダ３０１に公開鍵証明書データＣＥＲ$_{SP}$を送信する場合（図５８中（３））と、コンテンツプロバイダ３０１がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SP}$を取り寄せる場合（図５８中（１））とがある。

【０３４３】また、サービスプロバイダ３１０がコンテンツプロバイダ３０１の公開鍵証明書データＣＥＲ$_{CP}$を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ３０１からサービスプロバイダ３１０に公開鍵証明書データＣＥＲ$_{CP}$を送信する場合（図５８中（２））と、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{CP}$を取り寄せる場合（図５８中（４））とがある。

【０３４４】また、サービスプロバイダ３１０がＳＡＭ３０５$_1$～３０５$_4$の公開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_1$～３０５$_4$からサービスプロバイダ３１０に公開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$を送信する場合（図５８中（６））と、サービスプロバイダ

110

３１０がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$を取り寄せる場合（図５８中（４））とがある。

【０３４５】また、ＳＡＭ３０５$_1$～３０５$_4$がサービスプロバイダ３１０の公開鍵証明書データＣＥＲ$_{SP}$を取得する場合には、例えば、通信に先立ってサービスプロバイダ３１０からＳＡＭ３０５$_1$～３０５$_4$に公開鍵証明書データＣＥＲ$_{SP}$を送信する場合（図５８中（５））と、ＳＡＭ３０５$_1$～３０５$_4$がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SP}$を取り寄せる場合（図５８中（７）など）とがある。

【０３４６】また、ＳＡＭ３０５$_1$がＳＡＭ３０５$_2$の公開鍵証明書データＣＥＲ$_{SAM2}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_2$からＳＡＭ３０５$_1$に公開鍵証明書データＣＥＲ$_{SAM2}$を送信する場合（図５８中（８））と、ＳＡＭ３０５$_1$がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM2}$を取り寄せる場合（図５８中（７）など）とがある。

【０３４７】また、ＳＡＭ３０５$_2$がＳＡＭ３０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_1$からＳＡＭ３０５$_2$に公開鍵証明書データＣＥＲ$_{SAM1}$を送信する場合（図５８中（９））と、ＳＡＭ３０５$_2$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM1}$を取り寄せる場合と、ＳＡＭ３０５$_1$が搭載されたネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM1}$を取り寄せる場合（図５８中（７），（８））とがある。

【０３４８】また、ＳＡＭ３０５$_4$がＳＡＭ３０５$_{13}$の公開鍵証明書データＣＥＲ$_{SAM13}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_{13}$からＳＡＭ３０５$_4$に公開鍵証明書データＣＥＲ$_{SAM13}$を送信する場合（図５８中（１２））と、ＳＡＭ３０５$_4$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM13}$を取り寄せる場合（図５８中（１０））と、ユーザホームネットワーク３０３ｂ内のネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM13}$を取り寄せる場合とがある。

【０３４９】また、ＳＡＭ３０５$_{13}$がＳＡＭ３０５$_4$の公開鍵証明書データＣＥＲ$_{SAM4}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_4$からＳＡＭ３０５$_{13}$に公開鍵証明書データＣＥＲ$_{SAM4}$を送信する場合（図５８中（１１））と、ＳＡＭ３０５$_{13}$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM4}$を取り寄せる場合（図５８中（１３））と、ユーザホームネットワーク３０３ｂ内のネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM4}$を取り寄せる場合とがある。

【０３５０】第２実施形態における公開鍵証明書破棄リスト（データ）の取り扱い

第２実施形態では、ＥＭＤサービスセンタ３０２におい

て、不正行為などに用いられたコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０$5_1$～３０$5_4$が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データＣＲＬ(Certificate Revocation List)を、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０$5_1$～３０$5_4$に送信する。なお、公開鍵証明書破棄データＣＲＬは、ＥＭＤサービスセンタ３０２の他に、例えば、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０$5_1$～３０$5_4$において生成してもよい。

【０３５１】先ず、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１の公開鍵証明書データＣＥＲ$_{CP}$を無効にする場合について説明する。図５９に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{CP}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_1$をサービスプロバイダ３１０に送信する（図５９中（１））。サービスプロバイダ３１０は、コンテンツプロバイダ３０１から入力した署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_1$を参照して公開鍵証明書データＣＥＲ$_{CP}$の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{CP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ３０１からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【０３５２】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_1$を、サービスプロバイダ３１０の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えばＳＡＭ３０$5_1$に送信する（図５９中（１），（２））。ＳＡＭ３０$5_1$は、サービスプロバイダ３１０から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ３０１の署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_1$を参照して公開鍵証明書データＣＥＲ$_{CP}$の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{CP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。なお、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_1$を、ユーザホームネットワーク３０３内のネットワーク機器を介してＳＡＭ３０$5_1$に直接送信してもよい（図５９中（３））。

【０３５３】次に、ＥＭＤサービスセンタ３０２が、サービスプロバイダ３１０の公開鍵証明書データＣＥＲ$_{SP}$を無効にする場合について説明する。図６０に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{SP}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_2$をコンテンツプロバイダ３０１に送信する（図６０中（１））。コンテンツプロバイダ３０１は、サービスプロバイダ３１０から入力した署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_2$を参照して公開鍵証明書データＣＥＲ$_{SP}$の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{SP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ３１０からのデータを無効にする。

【０３５４】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_2$を、サービスプロバイダ３１０の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えばＳＡＭ３０$5_1$に送信する（図６０中（２））。ＳＡＭ３０$5_1$は、サービスプロバイダ３１０から入力したセキュアコンテナ内に格納されたサービスプロバイダ３１０の署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_2$を参照して公開鍵証明書データＣＥＲ$_{SP}$の有効性を判断し、有効であると判断した場合に公開鍵デー$K_{SP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。この場合に、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_2$の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_2$は、サービスプロバイダ３１０の関係者による改竄な困難な領域に格納される必要がある。なお、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_2$を、ユーザホームネットワーク３０３内のネットワーク機器を介してＳＡＭ３０$5_1$に直接送信してもよい（図６０中（３））。

【０３５５】次に、ＥＭＤサービスセンタ３０２が、例えばＳＡＭ３０$5_2$の公開鍵証明書データＣＥＲ$_{SAM2}$を無効にする場合について説明する。図６１に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{SAM2}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_3$をコンテンツプロバイダ３０１に送信する（図６１中（１））。コンテンツプロバイダ３０１は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０に送信する。サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えばＳＡＭ３０$5_1$に公開鍵証明書破棄データＣＲＬ$_{SAM1}$を送信する（図６１中（１））。ＳＡＭ３０$5_1$は、ＳＡＭ３０$5_2$から入力したデータに付加されたＳＡＭ３０$5_2$の署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_3$を参照して公開鍵証明書データＣＥＲ$_{SAM2}$の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{SAM2,P}$を用いた署名検証を行い、無

効であると判断した場合に当該署名検証を行わずに当該データを無効にする。この場合に、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_3$の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_3$は、サービスプロバイダ３１０の関係者による改竄な困難な領域に格納される必要がある。

【０３５６】ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０を介してＳＡＭ３０５$_1$に送信してもよい（図６１中（１），（２））。また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を、ユーザホームネットワーク３０３内のネットワーク機器を介してＳＡＭ３０５$_1$に直接送信してもよい（図６１中（３））。

【０３５７】また、ＥＭＤサービスセンタ３０２は、例えばＳＡＭ３０５$_2$の公開鍵証明書データＣＥＲ$_{SAM2}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_3$を作成し、これを保管する。また、ユーザホームネットワーク３０３は、バス１９１に接続されているＳＡＭのＳＡＭ登録リストＳＲＬを作成し、これをＥＭＤサービスセンタ３０２に送信する（図６２中（１））。ＥＭＤサービスセンタ３０２は、ＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定して新たなＳＡＭ登録リストＳＲＬを作成する。次に、ＥＭＤサービスセンタ３０２は、当該生成したＳＡＭ登録リストＳＲＬをＳＡＭ３０５$_1$に送信する（図６２中（１））。ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０３５８】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を作成し、これをコンテンツプロバイダ３０１に送信する（図６２中（２））。コンテンツプロバイダ３０１は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０に送信する（図６２中（２））。次に、サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データＣＲＬ$_3$をＳＡＭ３０５$_1$に送信する（図６２中（２））。ＳＡＭ３０５$_1$は、自らが作成したＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定する。以後、ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、当該ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０３５９】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を作成し、これをサービスプロバイダ３１０に送信する（図６２中（３））。次に、サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データＣＲＬ$_3$をＳＡＭ３０５$_1$に送信する（図６２中（３））。ＳＡＭ３０５$_1$は、自らが作成したＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定する。以後、ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、当該ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０３６０】ＥＭＤサービスセンタ３０２の役割等

図６３は、図３２に示すＥＭＤサービスセンタ（クリアリングハウス））３０２の機能を権利管理用クリアリングハウス９５０と、電子決済用クリアリングハウス９５１とに分割した場合のＥＭＤシステムの構成図である。当該ＥＭＤシステムでは、電子決済用クリアリングハウス９５１において、ユーザホームネットワーク３０３ａ，３０３ｂのＳＡＭからの利用履歴データ３０８に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ９０を介して決済機関９１において決済を行う。

【０３６１】また、権利管理用クリアリングハウス９５０は、電子決済用クリアリングハウス９５１からの決済通知に応じたコンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済レポートを作成し、それらをコンテンツプロバイダ３０１およびコンテンツプロバイダ３０１に送信する。また、コンテンツプロバイダ３０１の権利書データ１０６およびコンテンツ鍵データＫｃの登録（権威化）などを行う。なお、図６４に示すように、権利管理用クリアリングハウス９５０と電子決済用クリアリングハウス９５１とを単体の装置内に収納すると、図３２に示すＥＭＤサービスセンタ３０２となる。

【０３６２】また、本発明は、例えば、図６５に示すように、ＥＭＤサービスセンタ３０２に、権利管理用クリアリングハウス９６０の機能を設け、権利管理用クリアリングハウス９６０において、権利書データ１０６の登録などを行うと共に、ＳＡＭからの利用履歴データ３０８に基づいてサービスプロバイダ３１０の決済請求権データを作成し、これをサービスプロバイダ３１０に送信してもよい。この場合には、サービスプロバイダ３１０は、自らの課金システムを電子決済用クリアリングハウ

ス９６１として利用し、権利管理用クリアリングハウス９６０からの決済請求権データに基づいて決済を行う。

【０３６３】また、本発明は、例えば、図６６に示すように、ＥＭＤサービスセンタ３０２に、権利管理用クリアリングハウス９７０の機能を設け、権利管理用クリアリングハウス９７０において、権利書データ１０６の登録などを行うと共に、ＳＡＭからの利用履歴データ３０８に基づいてコンテンツプロバイダ３０１の決済請求権データを作成し、これをコンテンツプロバイダ３０１に送信してもよい。この場合には、コンテンツプロバイダ３０１は、自らの課金システムを電子決済用クリアリングハウス９６１として利用し、権利管理用クリアリングハウス９７０からの決済請求権データに基づいて決済を行う。

【０３６４】

【発明の効果】以上説明したように、本発明のデータ提供システムおよびその方法、管理装置並びにデータ処理装置によれば、データ処理装置においてデータ提供装置が提供した権利書データに基づいてコンテンツデータの利用が行われるため、データ提供装置の関係者の利益が適切に保護される。また、本発明のデータ提供システムおよびその方法と管理装置によれば、管理装置において権利書データなどの証明を行うため、例えば、権利書データなどが不正に改竄された場合などに適切に対処できる。また、本発明のデータ提供システムおよびその方法と管理装置によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

【図面の簡単な説明】

【図１】図１は、本発明の第１実施形態のＥＭＤシステムの全体構成図である。

【図２】図２は、図１に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのＳＡＭとの間で送受信されるデータに関連するデータの流れを示す図である。

【図３】図３は、図１に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとＥＭＤサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図４】図４は、図１に示すコンテンツプロバイダからＳＡＭに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図５】図５は、ＲＯＭ型の記録媒体を説明するための図である。

【図６】図６（Ａ）はコンテンツプロバイダからＥＭＤサービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図６（Ｂ）はＥＭＤサービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

【図７】図７は、図１に示すＥＭＤサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送

受信されるデータに関連するデータの流れを示す図である。

【図８】図８は、図１に示すＥＭＤサービスセンタの機能ブロック図であり、ＳＡＭおよび図１に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図９】図９は、図１に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図１０】図１０は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図１１】図１１は、図９に示す外部メモリに記憶されるデータを説明するための図である。

【図１２】図１２は、スタックメモリに記憶されるデータを説明するための図である。

【図１３】図１３は、図１に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図１４】図１４は、図１０に示す記憶部に記憶されるデータを説明するための図である。

【図１５】図１５は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図１６】図１６は、図９に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送元のＳＡＭ内での処理の流れを説明するための図である。

【図１７】図１７は、図１６に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図１８】図１８は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

【図１９】図１９は、図１６に示す場合において、転送先のＳＡＭにおいて、入力したコンテンツファイルなどを、ＲＡＭ型あるいはＲＯＭ型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図２０】図２０、コンテンツの購入形態が未決定の図５に示すＲＯＭ型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、ＡＶ機器において購入形態を決定する際の処理の流れを説明するための図である。

【図２１】図２１は、図２０に示す場合において、ＳＡＭ内でのデータの流れを示す図である。

【図２２】図２２は、ユーザホームネットワーク内のＡＶ機器において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナを読み出して、これを他のＡＶ機器に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図２３】図２３は、図２２に示す場合における転送元

のＳＡＭ内でのデータの流れを示す図である。

【図２４】図２４は、図２２に示す場合における転送先のＳＡＭ内でのデータの流れを示す図である。

【図２５】図２５は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図２６】図２６は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図２７】図２７は、バス１９１への機器の接続形態の一例を説明するための図である。

【図２８】図２８は、ＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図２９】図２９は、図１に示すコンテンツプロバイダの全体動作のフローチャートである。

【図３０】本発明の第１実施形態の第２変形例を説明するための図である。

【図３１】本発明の第１実施形態の第３変形例を説明するための図である。

【図３２】図３０は、本発明の第２実施形態のＥＭＤシステムの全体構成図である。

【図３３】図３３は、図３２に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図である。

【図３４】図３４は、図３２に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図３５】図３５は、図３２に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図３６】図３６は、図３２に示すサービスプロバイダの機能ブロック図であり、ＥＭＤサービスセンタとの間で送受信されるデータの流れを示す図である。

【図３７】図３７は、サービスプロバイダからＥＭＤサービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図３８】図３８は、図３２に示すＥＭＤサービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図３９】図３９は、図３２に示すＥＭＤサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図４０】図４０は、図３２に示すＥＭＤサービスセンタの機能ブロック図であり、ＳＡＭとの間で送受信されるデータに関連するデータの流れを示す図である。

【図４１】図４１は、利用履歴データの内容を説明するための図である。

【図４２】図４２は、図３２に示すネットワーク機器の構成図である。

【図４３】図４３は、図４２に示すＣＡモジュールの機能ブロック図である。

【図４４】図４４は、図４２に示すＳＡＭの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図４５】図４５は、図４４に示す記憶部に記憶されるデータを説明するための図である。

【図４６】図４６は、図４２に示すＳＡＭの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図４７】図４７は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図４８】図４８は、図４２に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送先のＳＡＭ内での処理の流れを説明するための図である。

【図４９】図４９は、図４８に示す場合の転送元のＳＡＭ内でのデータの流れを示す図である。

【図５０】図５０は、ネットワーク機器のＳＡＭからＡＶ機器のＳＡＭに転送される購入形態が既に決定されたセキュアコンテナのフォーマットを説明するための図である。

【図５１】図５１は、図４８に示す場合の転送先のＳＡＭ内でのデータの流れを示す図である。

【図５２】図５２は、図３２に示すＥＭＤシステムの全体動作のフローチャートである。

【図５３】図５３は、図３２に示すＥＭＤシステムの全体動作のフローチャートである。

【図５４】図５４は、本発明の第２実施形態の第１変形例に係わる２個のサービスプロバイダを用いたＥＭＤシステムの構成図である。

【図５５】図５５は、本発明の第２実施形態の第２変形例に係わる複数のコンテンツプロバイダを用いたＥＭＤシステムの構成図である。

【図５６】図５６は、本発明の第２実施形態の第３変形例に係わるＥＭＤシステムの構成図である。

【図５７】図５７は、本発明の第２実施形態の第４変形例に係わるＥＭＤシステムの構成図である。

【図５８】図５８は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図５９】図５９は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図６０】図６０は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図で

119

ある。

【図６１】図６１は、ＳＡＭの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図６２】図６２は、ＳＡＭの公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図６３】図６３は、図３２に示すＥＭＤシステムにおいて、ＥＭＤサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図６４】図６４は、図６３に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のＥＭＤサービスセンタ内に設けた場合のＥＭＤシステムの構成図である。

【図６５】図６５は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のＥＭＤシステムの構成図である。

【図６６】図６６は、コンテンツプロバイダが電子決済＊用クリアリングハウスに直接的に決済を行う場合のＥＭＤシステムの構成図である。

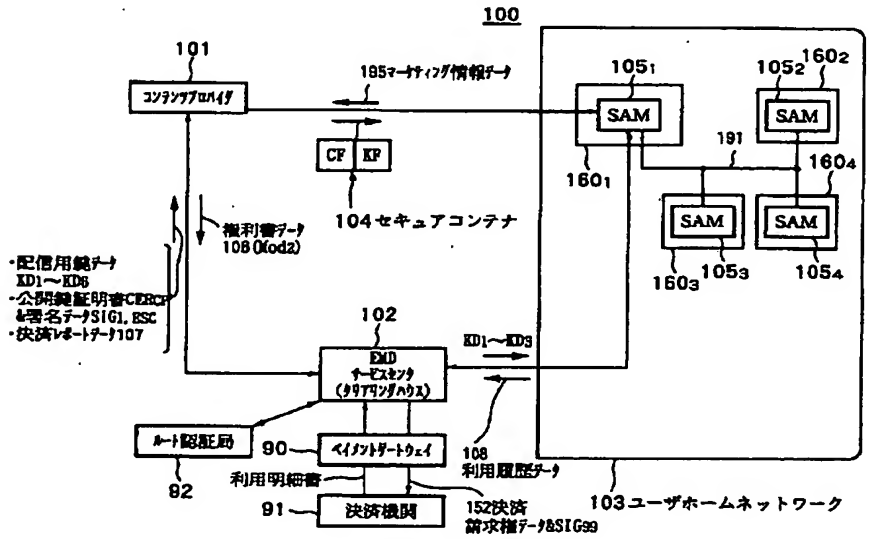
120

【図６７】従来のＥＭＤシステムの構成図である。

【符号の説明】

９０…ペイメントゲートウェイ、９１…決済機関、９２…ルート認証局、１００，３００…ＥＭＤシステム、１０１，３０１…コンテンツプロバイダ、１０２，３０２…ＥＭＤサービスセンタ、１０３，３０３…ユーザホームネットワーク、１０４，３０４…セキュアコンテナ、105_1～105_4，305_1～305_4…ＳＡＭ、１０６…権利書データ、１０７，３０７…決済レポートデータ、１０８，３０８…利用履歴データ、160_1…ネットワーク機器、160_2～160_4…ＡＶ機器、１５２，１５２ｃ，１５２ｓ…決済請求権データ、１９１…バス、３１０…サービスプロバイダ、３１１…ＣＡモジュール、３１２…プライスタグデータ、ＣＦ…コンテンツファイル、ＫＦ…キーファイル、Ｋｃ…コンテンツ鍵データ

【図１】

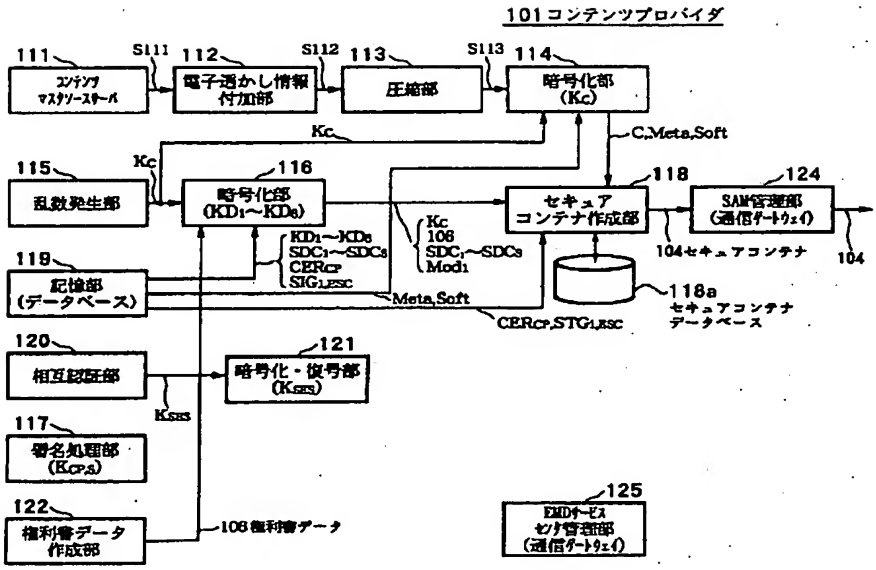


【図１１】

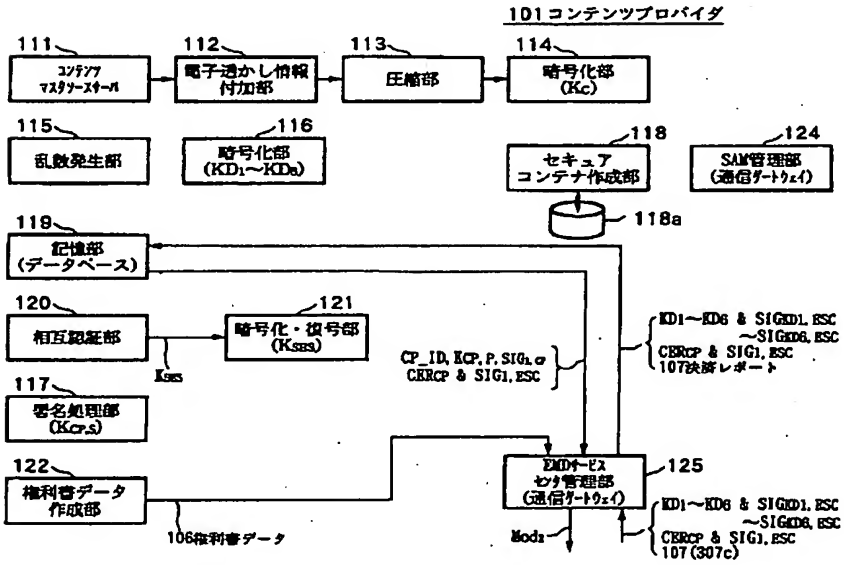
外部メモリ201に記憶されるデータ

利用履歴データ108
SAM登録リスト

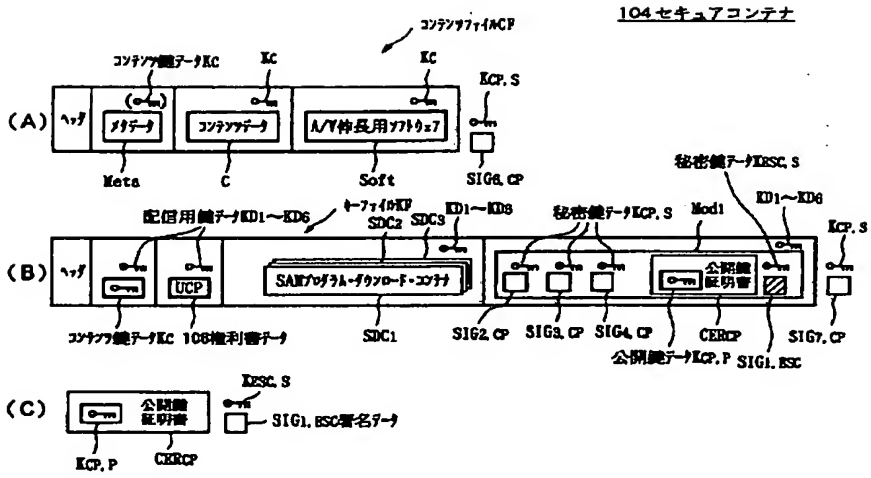
【図２】


101コンテンツプロバイダ
111
コンテンツマスタソースサーバ
S111
112
電子透かし情報付加部
S112
113
圧縮部
S113
114
暗号化部 (Kc)
Kc
C,Meta,Soft
115
乱数発生部
Kc
116
暗号化部 (KD1～KDs)
118
セキュアコンテナ作成部
124
SAM管理部 (通信ゲートウェイ)
104セキュアコンテナ
104
KD1～KDs
SDC1～SDCs
CERCP
SIG1,ESC
Kc
108
SDC1～SDCs
Mod1
119
記憶部 (データベース)
Meta,Soft
CERCP,STG1,ESC
118a
セキュアコンテナデータベース
120
相互認証部
121
暗号化・復号部 (KSES)
KSES
117
署名処理部 (KCP,S)
122
権利書データ作成部
108権利書データ
125
EMDサービスセンタ管理部 (通信ゲートウェイ)

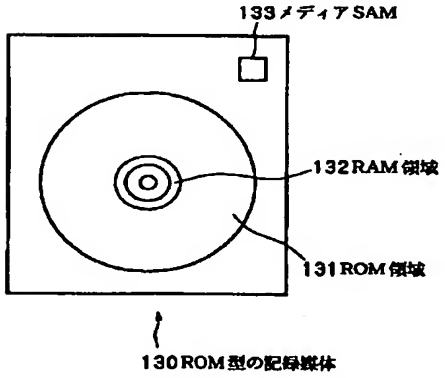
【図３】


101コンテンツプロバイダ
111
コンテンツマスタソースサーバ
112
電子透かし情報付加部
113
圧縮部
114
暗号化部 (Kc)
115
乱数発生部
116
暗号化部 (KD1～KDs)
118
セキュアコンテナ作成部
124
SAM管理部 (通信ゲートウェイ)
118a
119
記憶部 (データベース)
120
相互認証部
121
暗号化・復号部 (KSES)
KSES
CP_ID, KCP, P, SIG1, σ CERCP & SIG1, ESC
KD1～KD6 & SIGKD1, ESC ～SIGKD6, ESC
CERCP & SIG1, ESC
107決済レポート
117
署名処理部 (KCP,S)
122
権利書データ作成部
106権利書データ
125
EMDサービスセンタ管理部 (通信ゲートウェイ)
Mod1
KD1～KD6 & SIGKD1, ESC ～SIGKD6, ESC
CERCP & SIG1, ESC
107(307c)

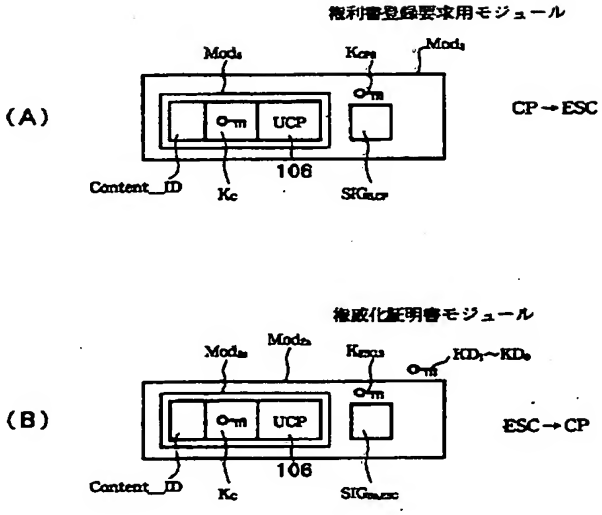
【図４】


104セキュアコンテナ
(A)
(B)
(C)
Meta
C
Soft
SIG6, CP
UCP
SAMプログラムダウンロード・コンテナ
SIG2, CP
SIG3, CP
SIG4, CP
CERCP
SIG7, CP
SIG1, ESC
KCP, P
SIG1, ESC署名データ

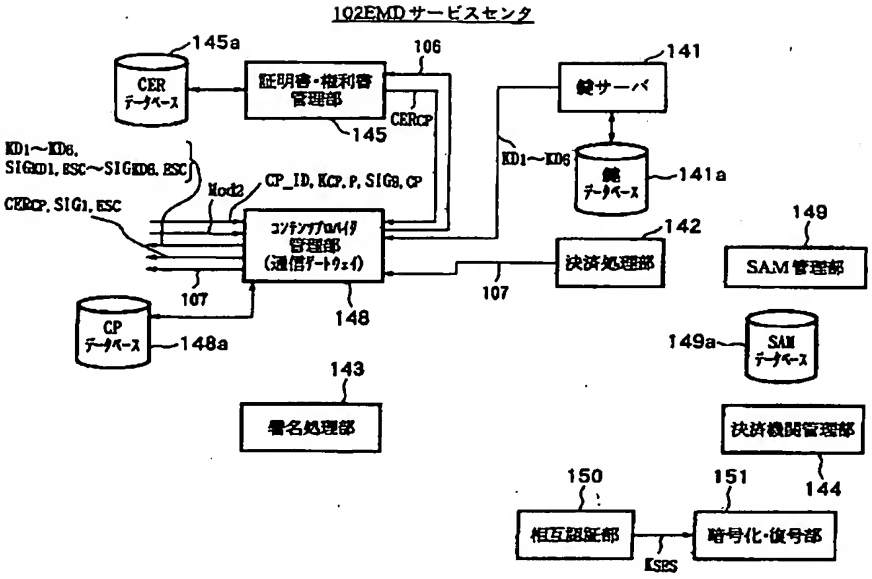
【図５】


133メディアSAM
132RAM領域
131ROM領域
130ROM型の記録媒体

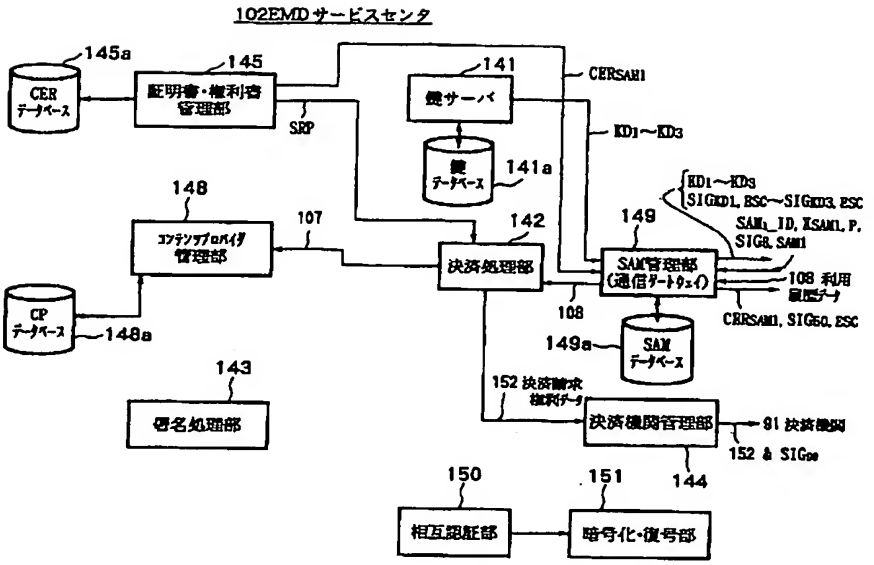
【図６】


権利書登録要求用モジュール
(A)
CP→ESC
UCP
106
Content_ID
Kc
権威化証明書モジュール
(B)
ESC→CP

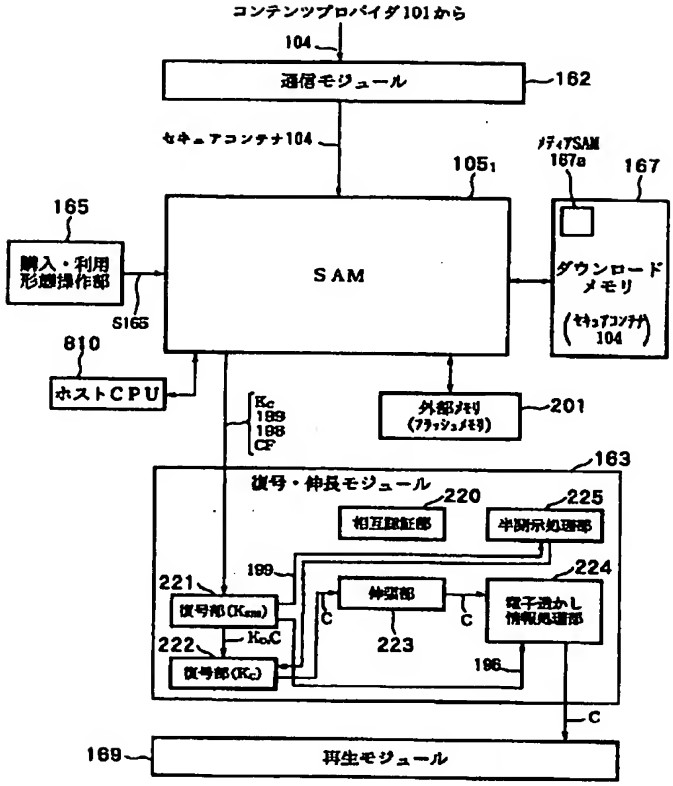
【図７】


102EMDサービスセンタ
145a
CER データベース
証明書・権利書 管理部
106
145
CERCP
鍵サーバ
141
KD1～KD6
鍵 データベース
141a
KD1～KD6, SIGKD1, ESC～SIGKD6, ESC
Mod2
CP_ID, KCP, P, SIG3, CP
CERCP, SIG1, ESC
コンテンツプロバイダ 管理部 (通信ゲートウェイ)
142
決済処理部
149
SAM管理部
107
107
148
CP データベース
148a
149a
SAM データベース
143
署名処理部
決済機関管理部
150
151
144
相互認証部
暗号化・復号部
KSES

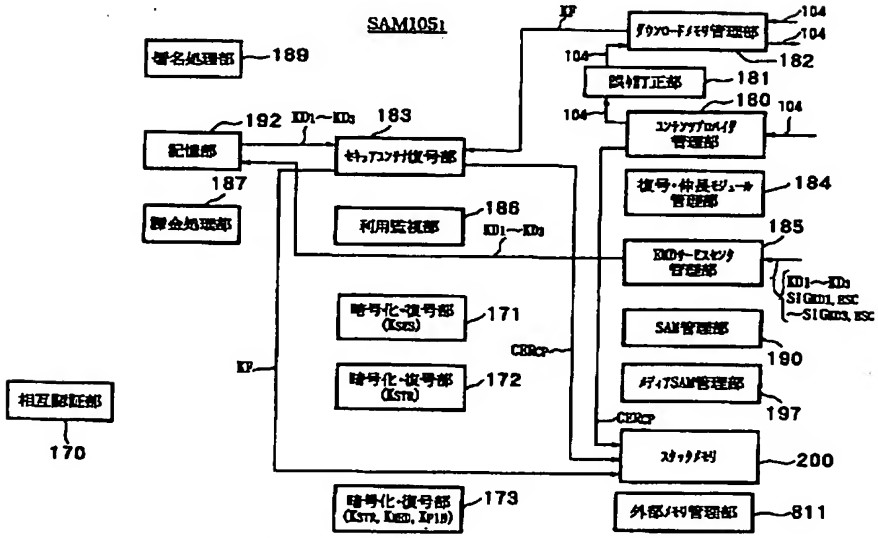
【図８】


102EMDサービスセンタ
145a
CER データベース
証明書・権利書 管理部
145
SRP
141
鍵サーバ
CERSAM1
KD1～KD3
鍵 データベース
141a
KD1～KD3 SIGKD1, ESC～SIGKD3, ESC
SAM1_ID, KSAM1, P, SIG3, SAM1
148
コンテンツプロバイダ 管理部
107
142
決済処理部
149
SAM管理部 (通信ゲートウェイ)
108 利用履歴データ
CERSAM1, SIG50, ESC
108
CP データベース
148a
149a
SAM データベース
143
署名処理部
152 決済請求 検証データ
決済機関管理部
91 決済機関
152 & SIG50
150
151
144
相互認証部
暗号化・復号部

【図９】



【図１０】

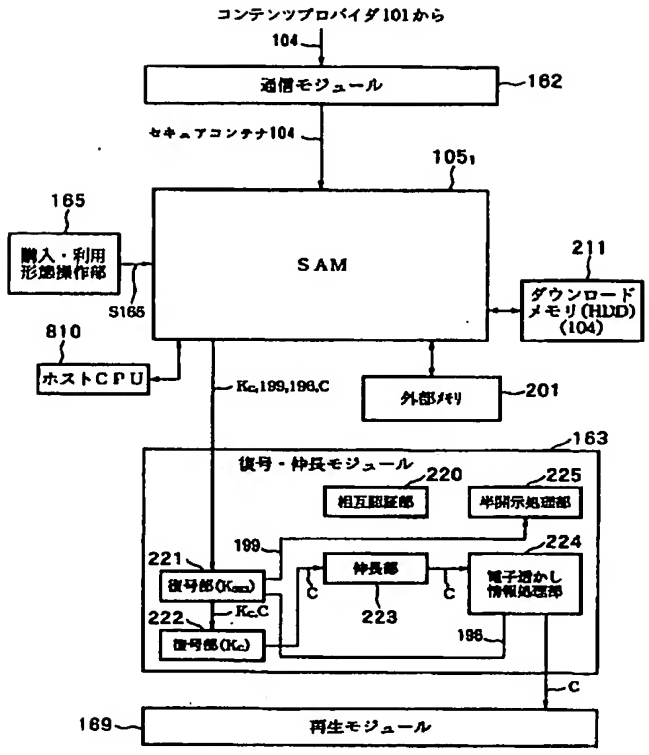


【図１２】

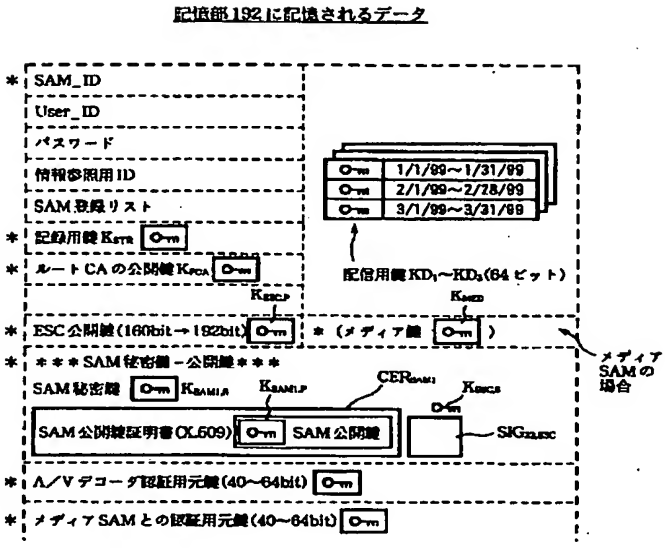
スタックメモリ200に記憶されるデータ

1　コンテンツ鍵データ Kc
権利書データ（UCP）106
記憶部（フラッシュメモリ）192のロック鍵データ K_{LOC}
コンテンツプロバイダ101の公開鍵証明書 $CERT_{CP}$
利用制御情状態データ（UCS）166
SAMプログラム・ダウンロード・コンテナ SD_1～SDC_3

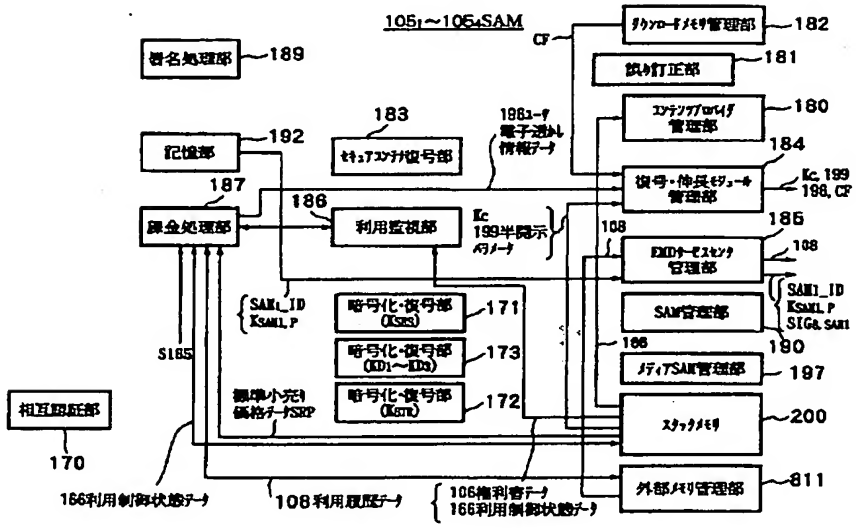
【図１３】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
105₁
165
購入・利用形態操作部
SAM
211
ダウンロードメモリ(HDD)(104)
S165
810
ホストCPU
Kc,199,198,C
外部メモリ
201
163
復号・伸長モジュール
220
相互認証部
225
半開示処理部
199
221
復号部(Kcnt)
伸長部
224
電子透かし情報処理部
222
Kc,C
223
復号部(Kc)
198
C
169
再生モジュール

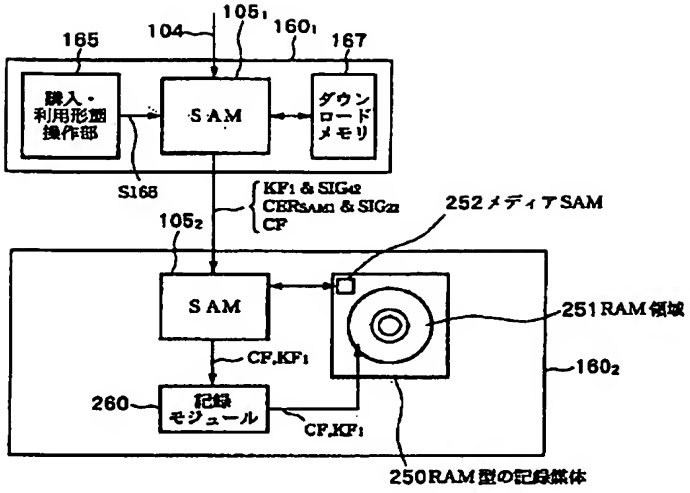
【図１４】


記憶部192に記憶されるデータ
SAM_ID
User_ID
パスワード
情報参照用ID
SAM登録リスト
記録用鍵 Kstr
ルートCAの公開鍵 KPCA
1/1/99～1/31/99
2/1/99～2/28/99
3/1/99～3/31/99
配信用鍵 KD1～KD3(64ビット)
KESCP
KMED
ESC公開鍵(160bit→192bit)
(メディア鍵)
メディアSAMの場合
＊＊＊SAM秘密鍵－公開鍵＊＊＊
SAM秘密鍵
KSAMI,S
KSAMI,P
CERSAM1
KESCS
SAM公開鍵証明書(X.509)
SAM公開鍵
SIGESC
Λ／Vデコーダ認証用元鍵(40～64bit)
メディアSAMとの認証用元鍵(40～64bit)

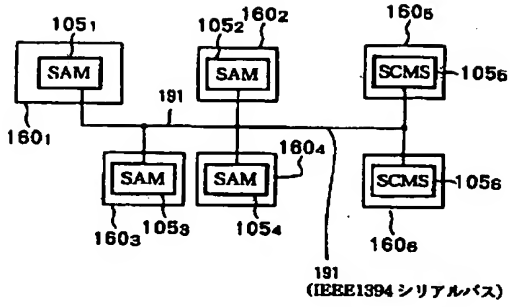
【図１５】


105₁～105₄SAM
CF
ダウンロードメモリ管理部
182
署名処理部
189
誤り訂正部
181
183
コンテンツプロバイダ管理部
180
記憶部
192
セキュアコンテナ復号部
電子透かし情報データ
184
復号・伸長モジュール管理部
Kc,199,198,CF
187
課金処理部
186
利用監視部
Kc,199半開示パラメータ
188
185
EKDサービスセンタ管理部
108
SAM1_ID
KSAM1,P
SAM管理部
SIG6,SAM1
166
190
メディアSAM管理部
197
暗号化・復号部(KSES)
171
暗号化・復号部(KD1～KD3)
173
暗号化・復号部(Kcnt)
172
スタックメモリ
200
S185
相互認証部
170
標準小売り価格データSKP
外部メモリ管理部
811
166利用制御状態データ
108利用履歴データ
106権利書データ
166利用制御状態データ

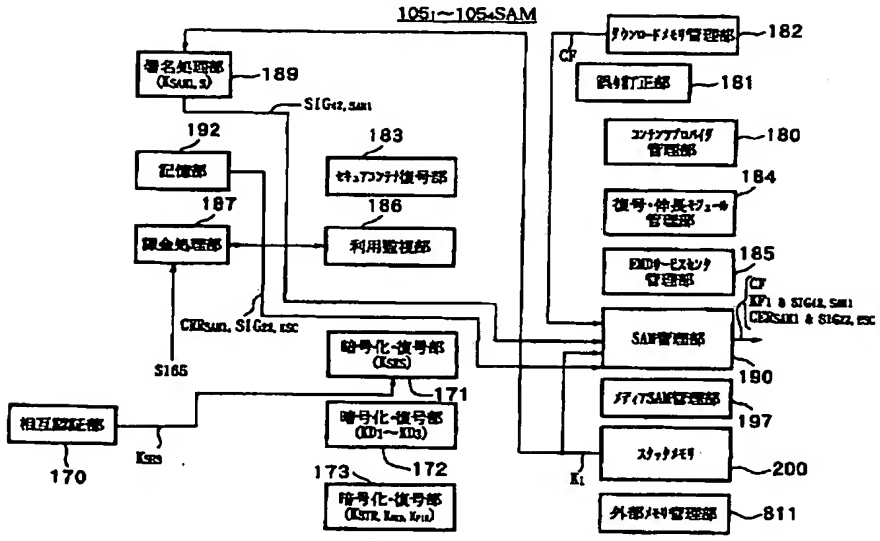
【図１６】


165
104
105_1
160_1
167
購入・利用形態操作部
SAM
ダウンロードメモリ
S168
KF_1 & SIG_{42}
CER_{SAM1} & SIG_{22}
CF
105_2
252メディアSAM
SAM
251RAM領域
CF,KF_1
160_2
260
記録モジュール
CF,KF_1
250RAM型の記録媒体

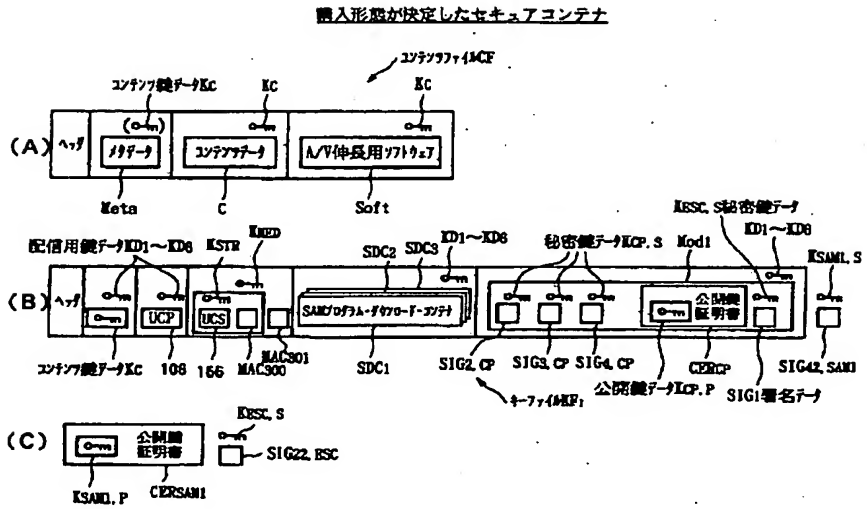
【図２７】


105_1
105_2
160_2
160_5
SAM
SAM
SCMS
105_5
191
160_1
SAM
SAM
160_4
SCMS
105_6
160_3
105_3
105_4
160_6
191
(IEEE1394シリアルバス)

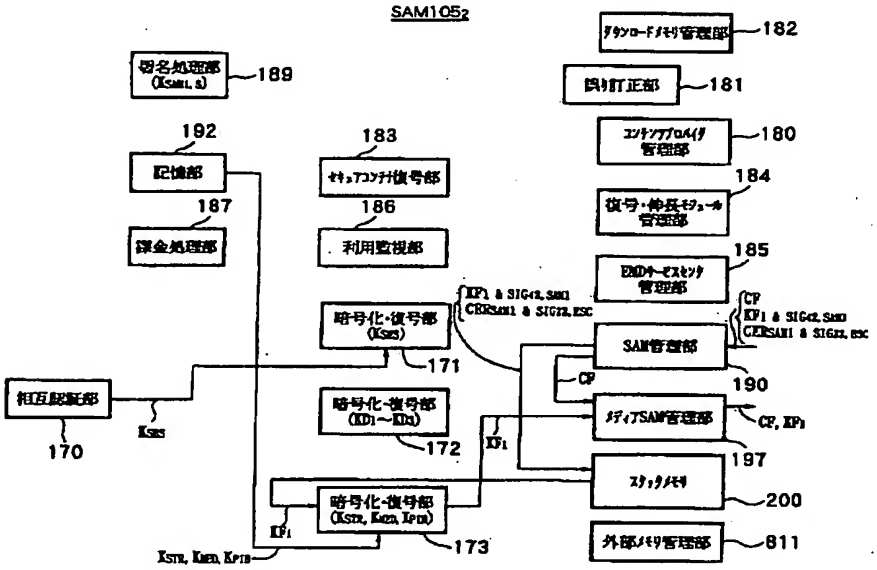
【図１７】


105_1～105_4SAM
署名処理部
189
$SIG_{42, SAM1}$
192
記憶部
183
187
186
課金処理部
利用監視部
CER_{SAM1}, $SIG_{22, ESC}$
S165
暗号化・復号部
171
相互認証部
170
K_{SES}
暗号化・復号部
173
172
182
CF
鍵修正部
181
180
184
185
CF
KF_1 & $SIG_{42, SAM1}$
CER_{SAM1} & $SIG_{22, ESC}$
SAM管理部
190
197
K_1
200
811

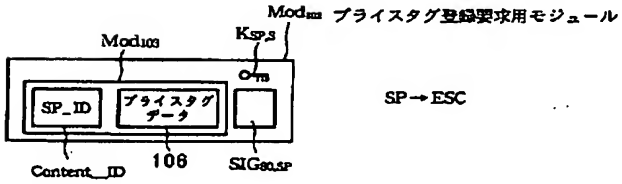
【図１８】


購入形態が決定したセキュアコンテナ
(A)
(B)
(C)
Meta
C
Soft
SDC1
SDC2
SDC3
MAC300
MAC301
SIG1署名データ
SIG2, CP
SIG3, CP
SIG4, CP
SIG42, SAM1
SIG22, ESC
KSAM1, P
CERSAM1

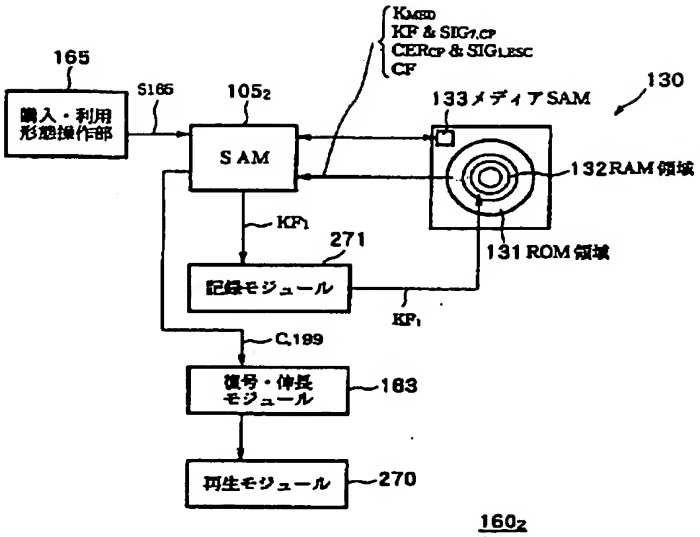
【図１９】


SAM105₂
189
182
181
180
192
183
184
187
186
185
171
190
170
172
197
200
173
811

【図３７】


Mod₁₀₂ プライスタグ登録要求用モジュール
Mod₁₀₃
SP_ID
プライスタグデータ
106
SP→ESC

【図２０】

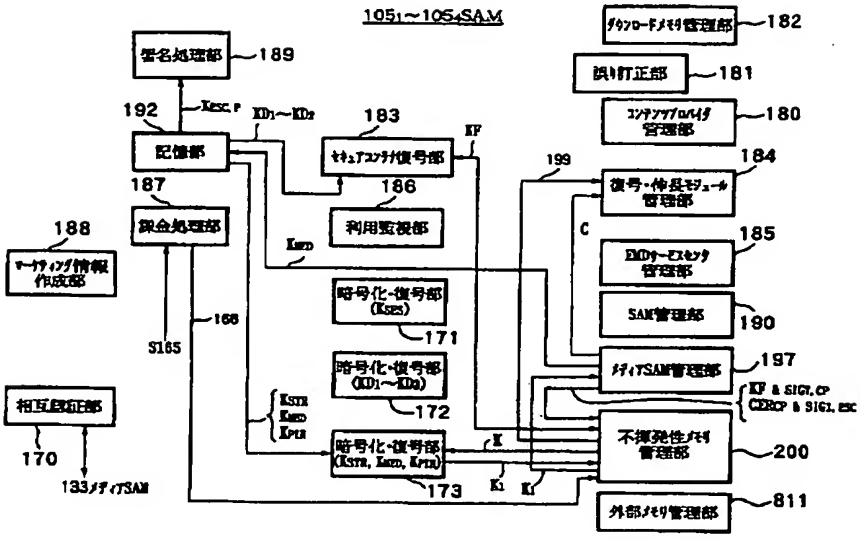


【図４１】

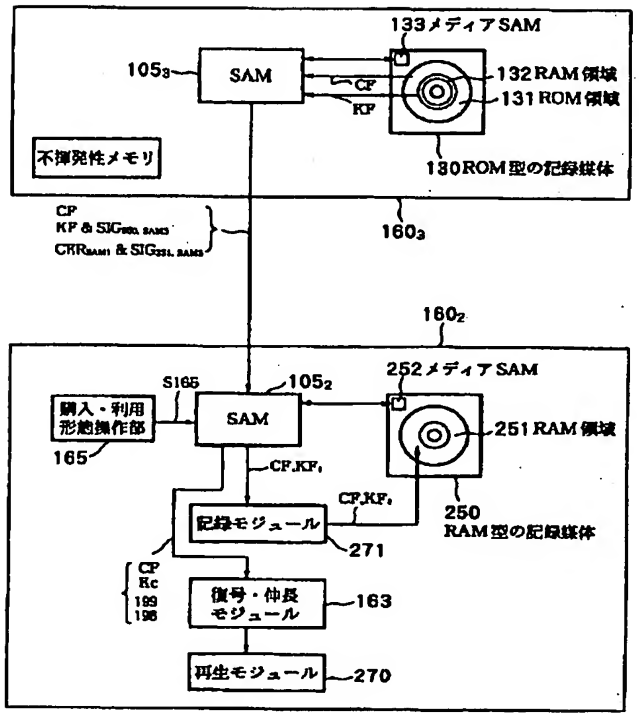
利用履歴データ308の内容

識別子Content_ID
識別子CP_ID
識別子SP_ID
コンテンツデータCの信号諸元データ
コンテンツデータCの圧縮方法
記録媒体の識別子Media_ID
識別子SAM_ID、
ユーザのUSER_ID

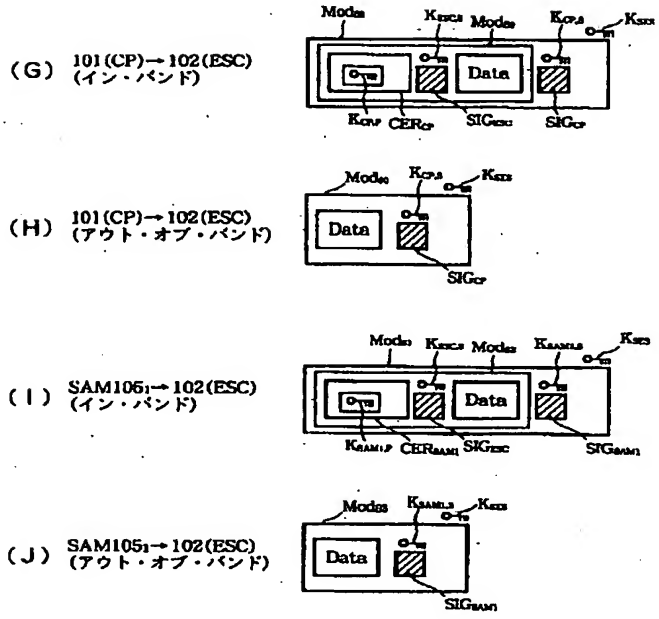
【図２１】



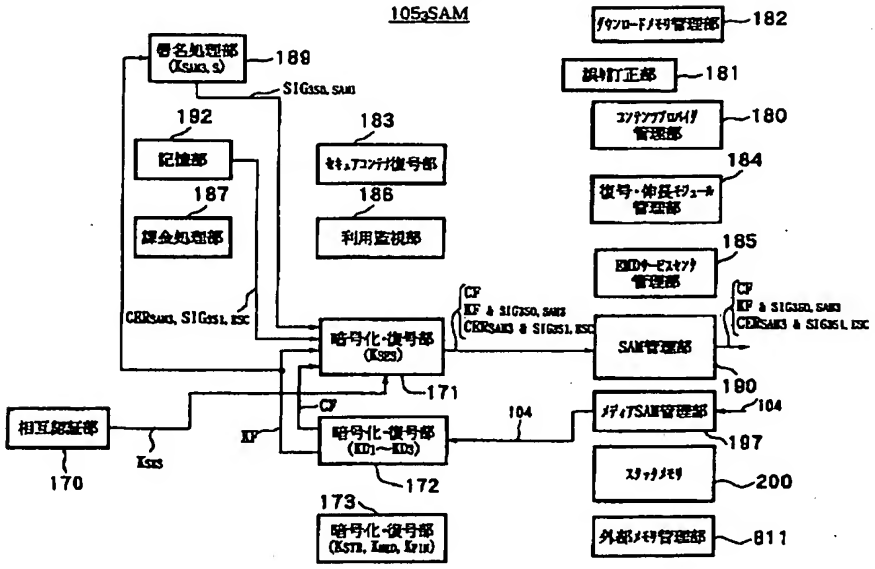
【図２２】


133メディアSAM
105₃
SAM
CP
KP
132 RAM領域
131 ROM領域
不揮発性メモリ
130 ROM型の記録媒体
CP
KP & SIG
CERSAM1 & SIG
160₃
160₂
252メディアSAM
S165
105₂
SAM
購入・利用形態操作部
165
251 RAM領域
CP,KF,
CP,KF,
250
RAM型の記録媒体
記録モジュール
271
CP
Kc
199
198
復号・伸長モジュール
163
再生モジュール
270

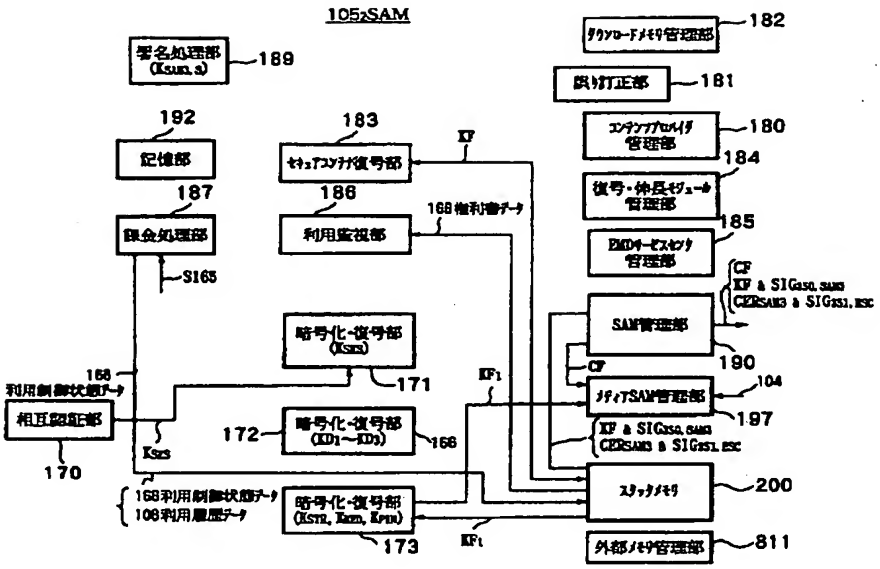
【図２６】


(G) 101(CP)→102(ESC)
(イン・バンド)
Mode
Data
(H) 101(CP)→102(ESC)
(アウト・オブ・バンド)
Data
(I) SAM105₁→102(ESC)
(イン・バンド)
Data
(J) SAM105₁→102(ESC)
(アウト・オブ・バンド)
Data

【図２３】


105₂SAM
署名処理部
189
SIG
192
記憶部
187
課金処理部
183
186
利用監視部
CERSAM3, SIG
暗号化・復号部
171
CP
CP
KF & SIG
CERSAM3 & SIG
SAM管理部
190
相互認証部
170
KSES
KF
暗号化・復号部
172
104
104
メディアSAM管理部
187
200
173
暗号化・復号部
811
182
181
180
184
185

【図２４】

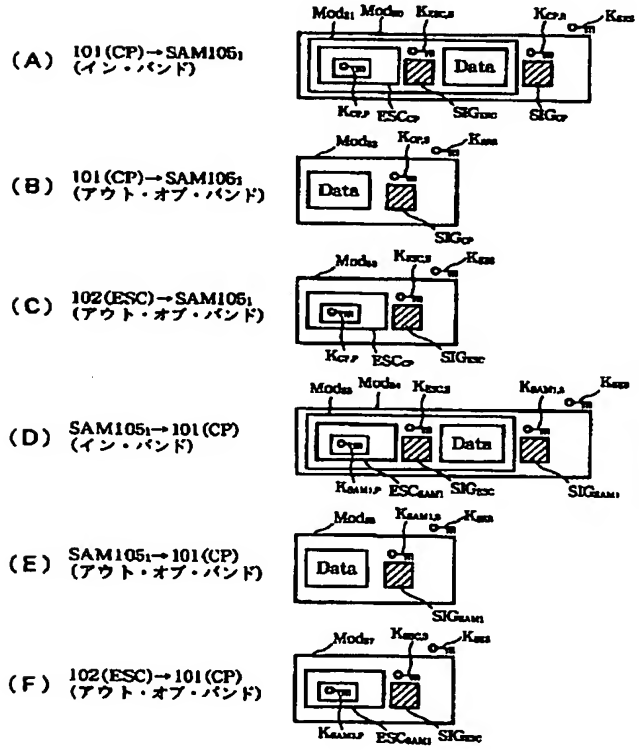


【図４５】

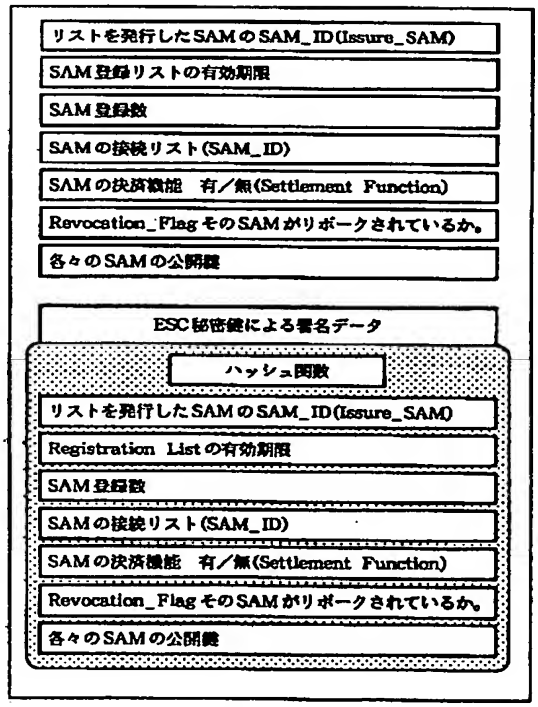
スタックメモリ200の記憶データ

コンテンツ鍵データ Kc
権利書データ（UCP）106
不揮発性メモリ201のロック鍵データ K_{LOC}
コンテンツプロバイダ301の公開鍵証明書データ CER_{CP}
サービスプロバイダ301の公開鍵証明書データ CER_{SP}
利用制御情状態データ（UCS）166
SAMプログラム・ダウンロード・コンテナ SD_1～SDC_n
プライスタグデータ312

【図２５】

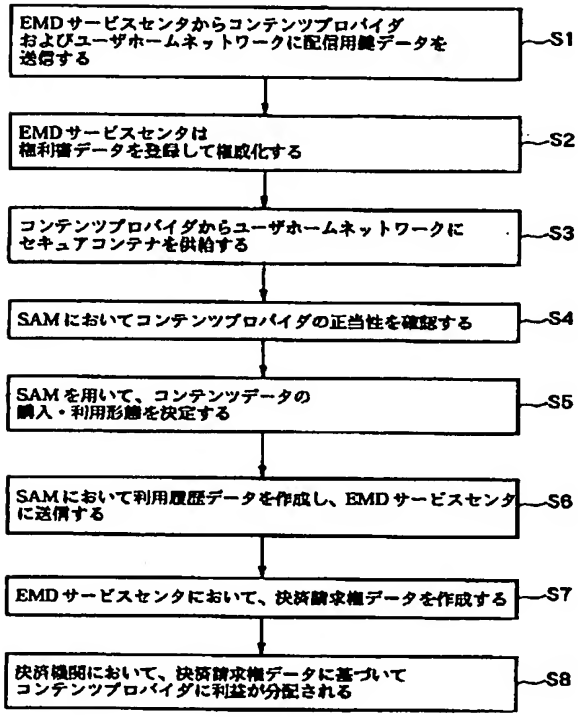


【図２８】

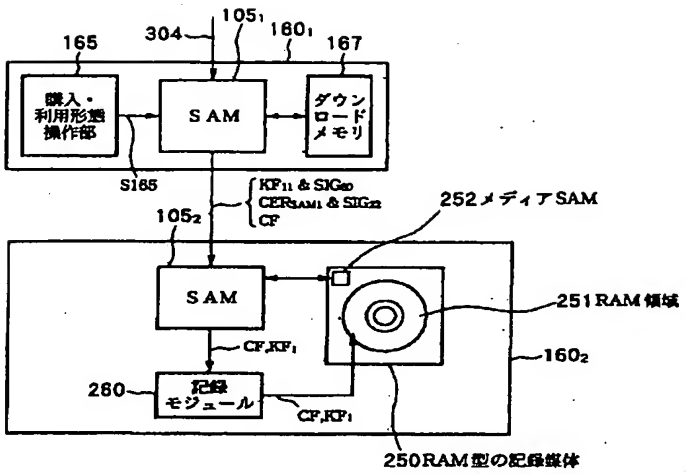


SAM登録リスト

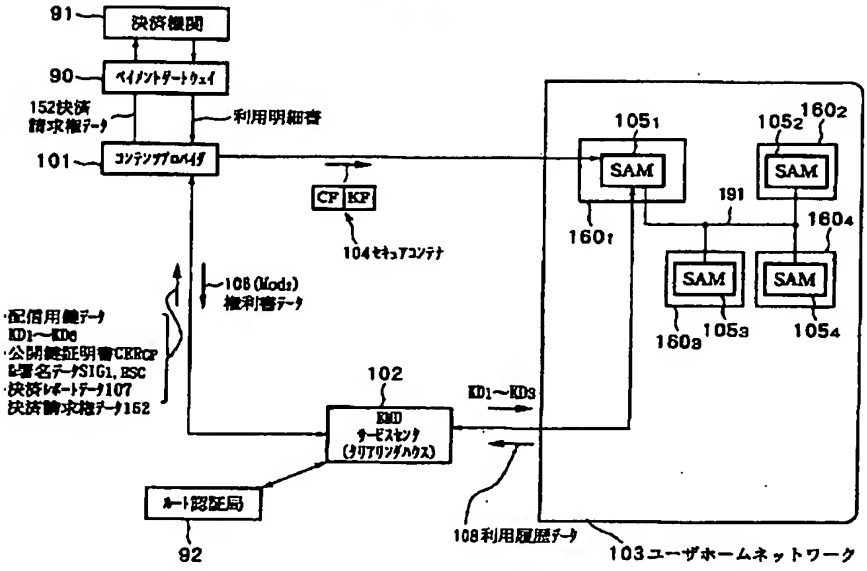
【図２９】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークに配信用鍵データを送信する
S1
EMDサービスセンタは権利書データを登録して権威化する
S2
コンテンツプロバイダからユーザホームネットワークにセキュアコンテナを供給する
S3
SAMにおいてコンテンツプロバイダの正当性を確認する
S4
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S5
SAMにおいて利用履歴データを作成し、EMDサービスセンタに送信する
S6
EMDサービスセンタにおいて、決済請求権データを作成する
S7
決済機関において、決済請求権データに基づいてコンテンツプロバイダに利益が分配される
S8

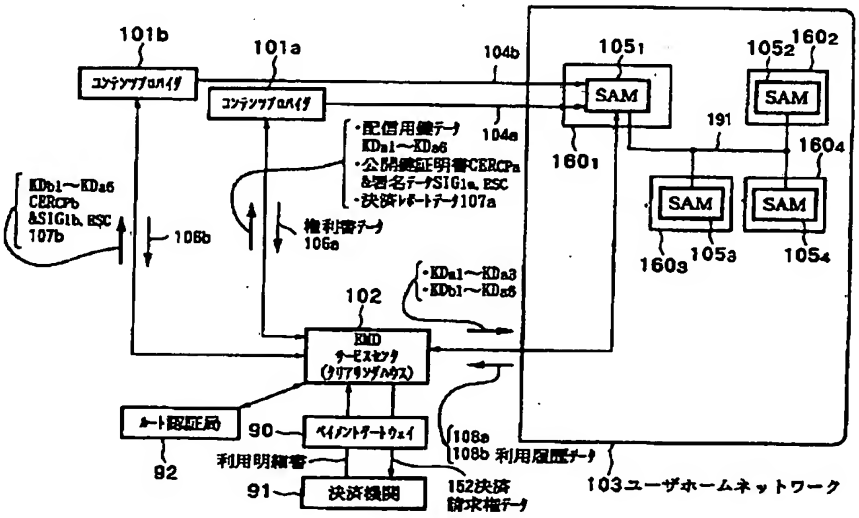
【図４８】


165
304
105_1
160_1
167
購入・利用形態操作部
SAM
ダウンロードメモリ
S165
KF_{11} & SIG_{ID}
CER_{SAM1} & SIG_{22}
CF
105_2
252メディアSAM
SAM
251RAM領域
CF,KF_1
160_2
280
記録モジュール
CF,KF_1
250RAM型の記録媒体

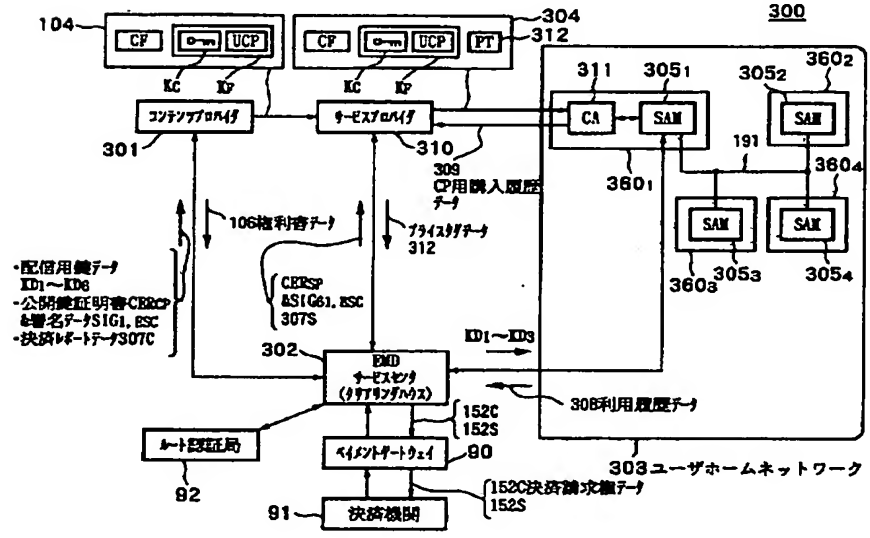
【図３０】


91
決済機関
90
ペイメントゲートウェイ
152決済請求権データ
利用明細書
101
コンテンツプロバイダ
CF KF
104セキュアコンテナ
108(Mods)権利書データ
配信用鍵データ
KD1～KDn
公開鍵証明書CERCP
E-署名データSIG1, ESC
決済レポートデータ107
決済請求権データ152
102
EMDサービスセンタ(タリアリングハウス)
KD1～KDn
ルート認証局
92
105_1
105_2
160_2
SAM
SAM
191
160_1
160_4
SAM
SAM
160_3
105_3
105_4
108利用履歴データ
103ユーザホームネットワーク

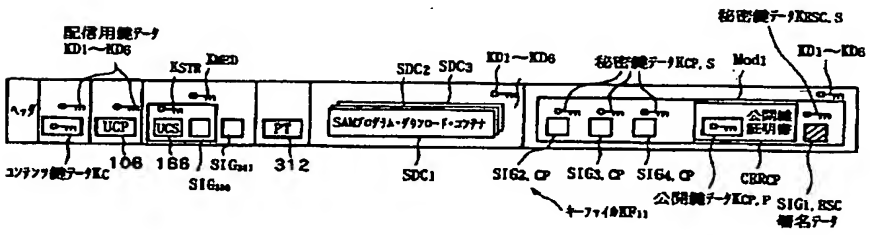
【図３１】


101b
101a
104b
SAM
SAM
SAM
SAM
SAM
191
160₄
160₃
105₃
105₄
KDb1～KDa6
CERCPb
&SIG1b, ESC
107b
108b
104a
・配信用鍵データ
KDa1～KDa6
・公開鍵証明書CERCPa
&署名データSIG1a, ESC
・決済レポートデータ107a
権利書データ
106a
・KDa1～KDa3
・KDb1～KDa6
102
EMD
サービスセンタ
(クリアリングハウス)
ルート認証局
90
ペイメントゲートウェイ
92
利用明細書
91
決済機関
108a
108b 利用履歴データ
152決済
請求権データ
103ユーザホームネットワーク

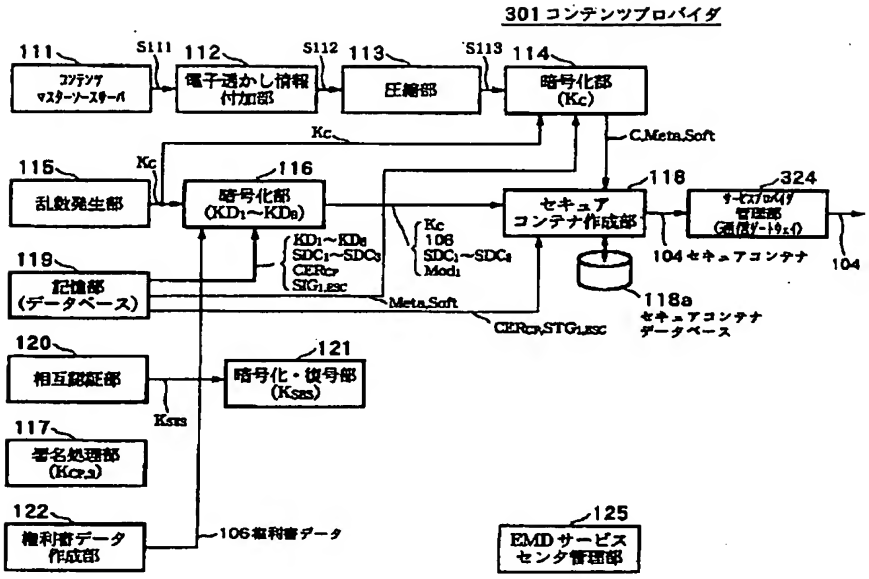
【図３２】


104
CF
UCP
PT
304
312
KC
KF
300
311
CA
SAM
191
360₄
360₃
305₃
305₄
コンテンツプロバイダ
サービスプロバイダ
301
310
309
CP用購入履歴
データ
106権利書データ
プライスタグデータ
312
・配信用鍵データ
KD1～KD6
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ307C
CERSP
&SIG61, ESC
307S
KD1～KD3
302
EMD
サービスセンタ
(クリアリングハウス)
308利用履歴データ
152C
152S
ルート認証局
90
ペイメントゲートウェイ
92
303ユーザホームネットワーク
152C決済請求権データ
152S
91
決済機関

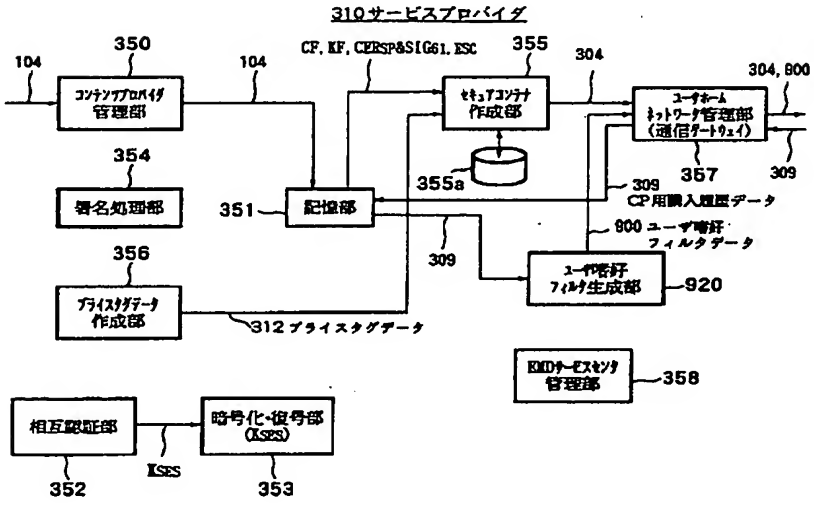
【図４７】


配信用鍵データ
KD1～KD6
KSTR
EMED
SDC2
SDC3
KD1～KD6
秘密鍵データKCP, S
Mod1
秘密鍵データKESC, S
KD1～KD6
ヘッダ
UCP
UCS
PT
公開鍵証明書
コンテンツ鍵データKC
106
108
SIG1
SIG100
312
SDC1
SIG2, CP
SIG3, CP
SIG4, CP
CERCP
公開鍵データKCP, P
SIG1, ESC
署名データ

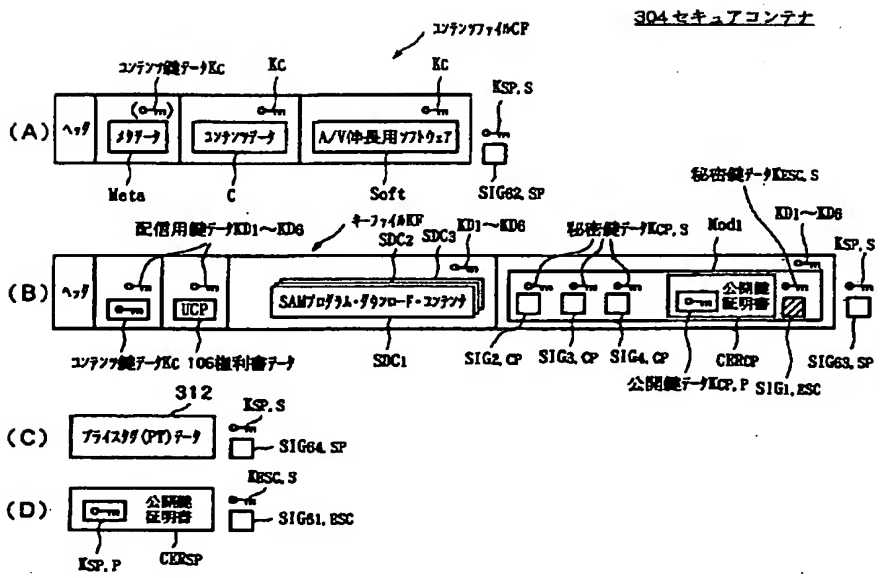
【図３３】


301コンテンツプロバイダ
111
S111
112
S112
113
S113
114
電子透かし情報付加部
圧縮部
暗号化部 (Kc)
Kc
C,Meta,Soft
115
乱数発生部
116
暗号化部 (KD1～KD8)
118
セキュアコンテナ作成部
324
104セキュアコンテナ
104
119
記憶部 (データベース)
KD1～KD8
SDC1～SDC8
CERCP
SIG1,ESC
Kc
106
SDC1～SDC8
Mod1
Meta,Soft
CERCP,STG1,ESC
118a
セキュアコンテナデータベース
120
相互認証部
121
暗号化・復号部 (KSES)
KSES
117
署名処理部 (KCP,S)
122
権利書データ作成部
106権利書データ
125
EMDサービスセンタ管理部

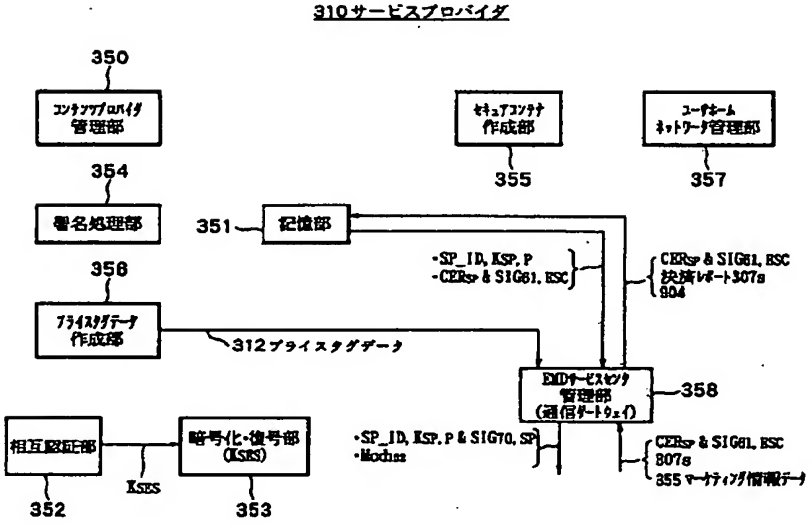
【図３４】


310サービスプロバイダ
104
350
コンテンツプロバイダ管理部
104
CF, KF, CERSP&SIG61, ESC
355
セキュアコンテナ作成部
304
304, 800
ユーザホームネットワーク管理部 (通信ゲートウェイ)
357
309
354
署名処理部
351
記憶部
355a
309
CP用購入履歴データ
800 ユーザ嗜好フィルタデータ
356
プライスタグデータ作成部
312プライスタグデータ
309
ユーザ嗜好フィルタ生成部
920
EMDサービスセンタ管理部
358
相互認証部
352
KSES
暗号化・復号部 (KSES)
353

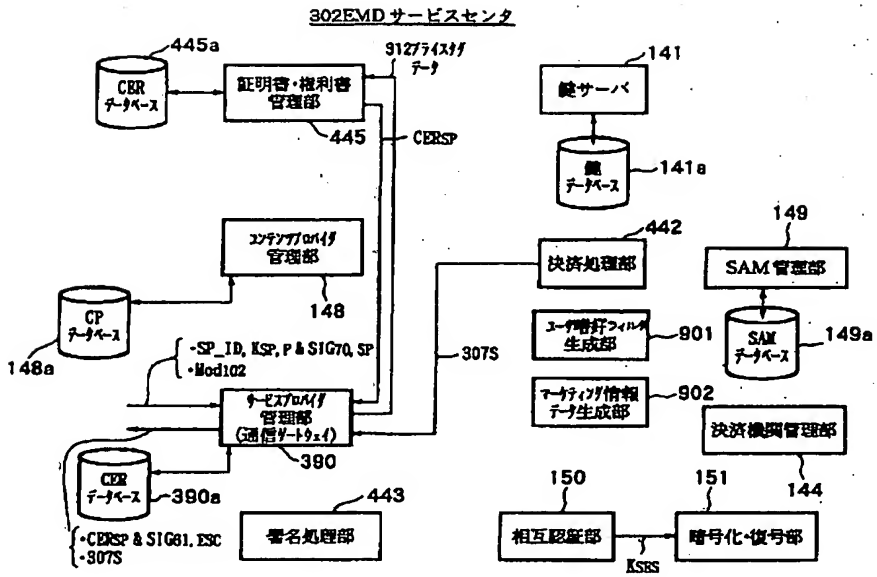
【図３５】


304 セキュアコンテナ
コンテンツファイルCF
コンテンツ鍵データKc
Kc
Kc
KSP, S
(A)
ヘッダ
メタデータ
コンテンツデータ
A/V伸長用ソフトウェア
Meta
C
Soft
SIG62, SP
秘密鍵データKESC, S
KD1～KD6
配信用鍵データKD1～KD6
キーファイルKF
SDC2
SDC3
KD1～KD6
秘密鍵データKCP, S
Mod1
KSP, S
(B)
ヘッダ
UCP
SAMプログラム・ダウンロード・コンテンツ
公開鍵証明書
コンテンツ鍵データKc
106権利書データ
SDC1
SIG2, CP
SIG3, CP
SIG4, CP
CERCP
公開鍵データKCP, P
SIG1, ESC
SIG63, SP
312
KSP, S
(C)
プライスタグ(PT)データ
SIG64, SP
KESC, S
(D)
公開鍵証明書
SIG61, ESC
KSP, P
CERSP

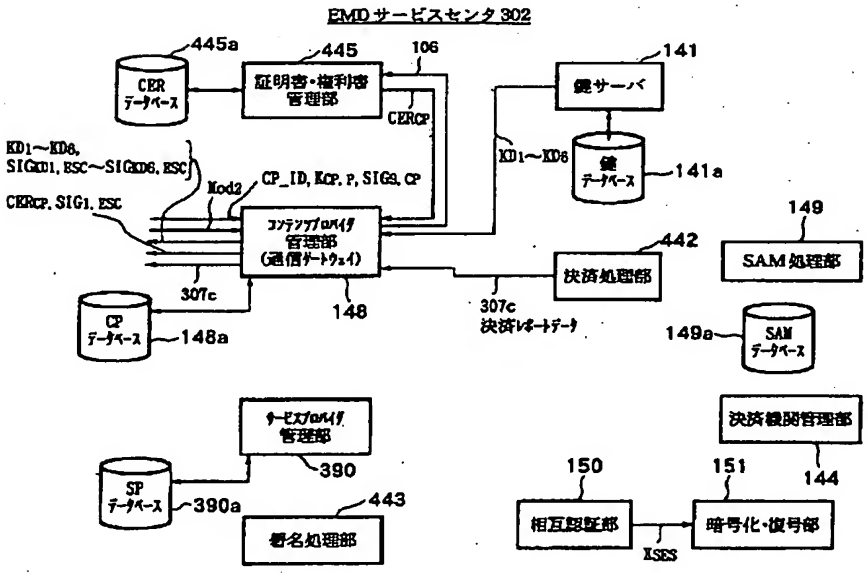
【図３６】


310サービスプロバイダ
350
コンテンツプロバイダ管理部
セキュアコンテナ作成部
ユーザホームネットワーク管理部
354
355
357
署名処理部
351
記憶部
・SP_ID, KSP, P
・CERSP & SIG61, ESC
CERSP & SIG61, ESC
決済レポート307a
904
356
プライスタグデータ作成部
312プライスタグデータ
EMDサービスセンタ管理部(通信ゲートウェイ)
358
相互認証部
暗号化・復号部(KSRS)
KSES
・SP_ID, KSP, P & SIG70, SP
・Mochiss
CERSP & SIG61, ESC
307a
355 マーケティング情報データ
352
353

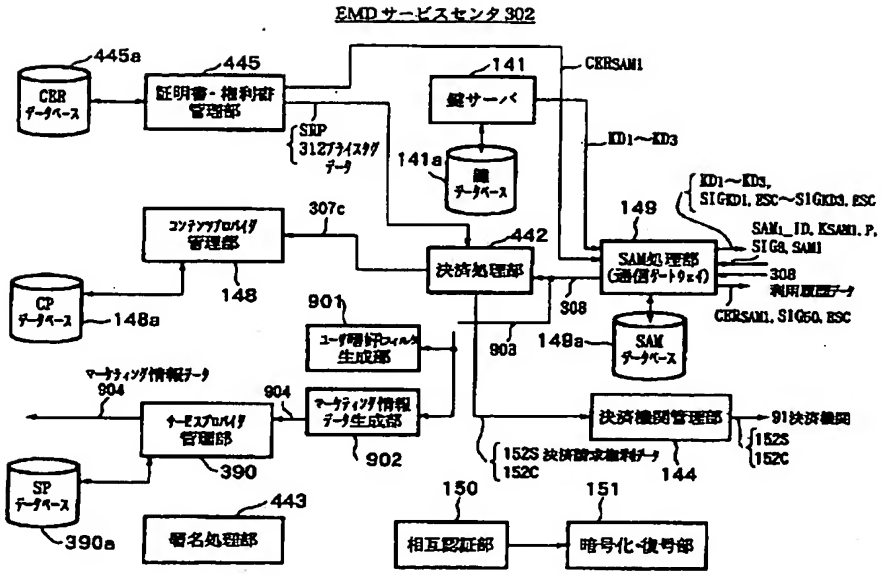
【図３８】


302EMDサービスセンタ
445a
CER データベース
証明書・権利書管理部
445
CERSP
141
鍵サーバ
141a
鍵データベース
442
決済処理部
149
SAM管理部
149a
SAM データベース
901
902
決済機関管理部
144
150
151
相互認証部
暗号化・復号部
KSES
148
CP データベース
148a
307S
390
390a
443
署名処理部

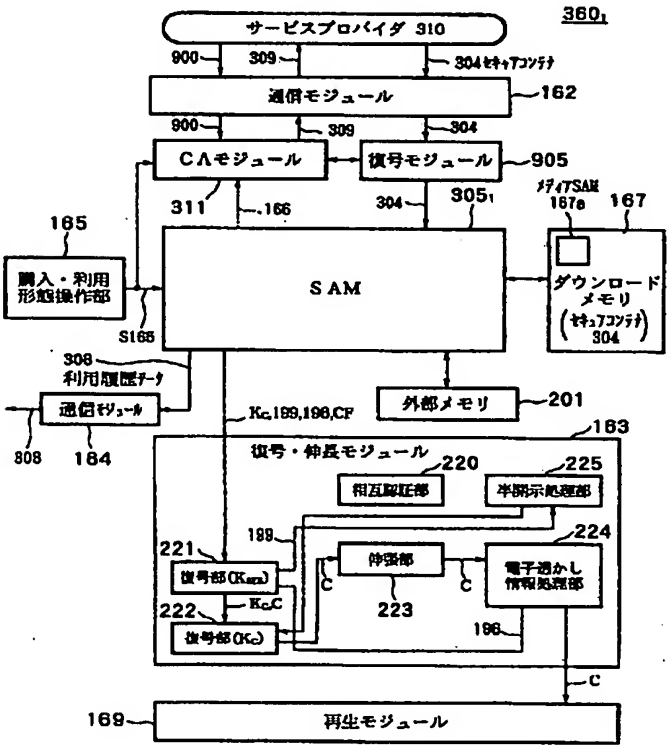
【図３９】


EMDサービスセンタ302
445a
CER データベース
445
証明書・権利書管理部
106
CERCP
141
鍵サーバ
141a
鍵データベース
442
決済処理部
149
SAM処理部
149a
SAM データベース
148
CP データベース
148a
307c
390
390a
443
署名処理部
150
151
144
相互認証部
暗号化・復号部
KSES

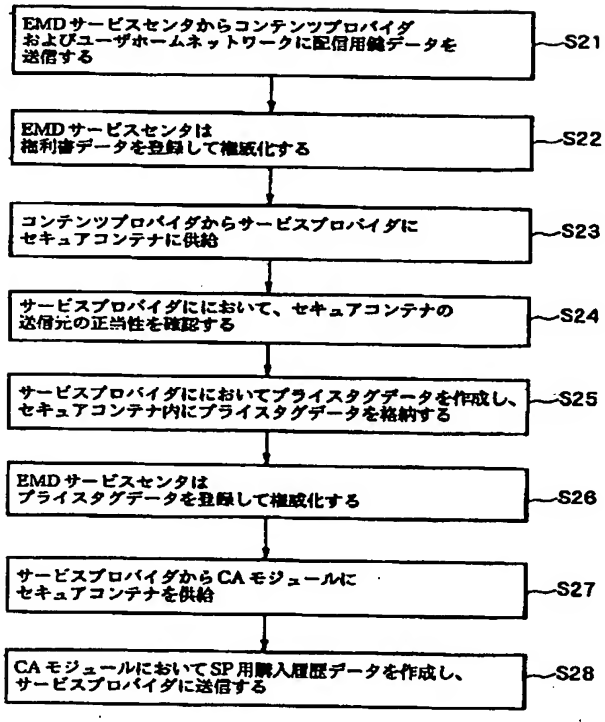
【図４０】


EMDサービスセンタ302
445a
CER データベース
445
証明書・権利書管理部
141
鍵サーバ
CERSAM1
SKP 312プライスタグデータ
141a
鍵データベース
KD1～KD3
KD1～KD3, SIGKD1, ESC～SIGKD3, ESC
149
SAM1_ID, KSAM1, P, SIG3, SAM1
307c
コンテンツプロバイダ管理部
442
決済処理部
SAM処理部(通信ゲートウェイ)
308
利用履歴データ
CERSAM1, SIG50, ESC
CP データベース
148
148a
901
ユーザ嗜好フィルタ生成部
903
149a
SAM データベース
マーケティング情報データ
904
904
サービスプロバイダ管理部
マーケティング情報データ生成部
902
決済機関管理部
91決済機関
152S 決済請求権利データ
152C
152S
152C
144
390
SP データベース
390a
443
署名処理部
150
相互認証部
151
暗号化・復号部

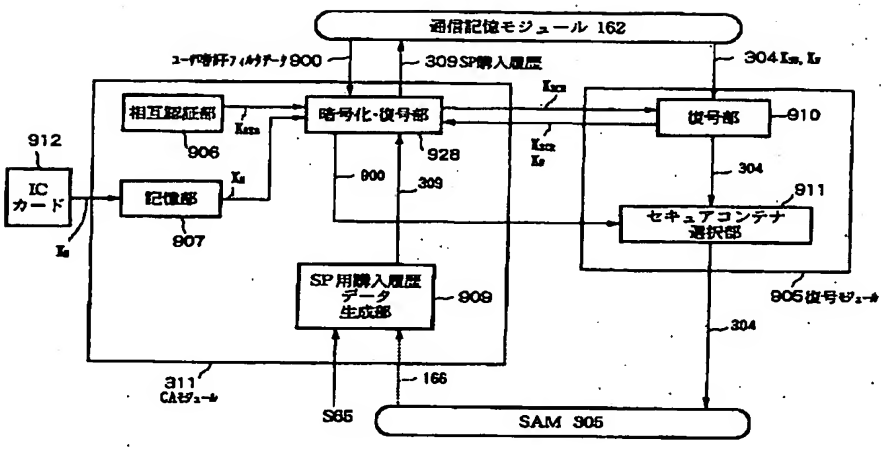
【図４２】


360₁
サービスプロバイダ 310
900
309
304 セキュアコンテナ
通信モジュール
162
900
309
304
CAモジュール
復号モジュール
905
311
166
304
305₁
メディアSAM 167a
167
165
購入・利用形態操作部
SAM
ダウンロードメモリ (セキュアコンテナ) 304
S165
308 利用履歴データ
通信モジュール
外部メモリ
201
Kc,199,196,CF
163
308
184
復号・伸長モジュール
相互認証部
220
半開示処理部
225
199
224
221
伸張部
電子透かし情報処理部
復号部(Kmn)
C
C
223
222
KcC
復号部(Kc)
196
C
169
再生モジュール

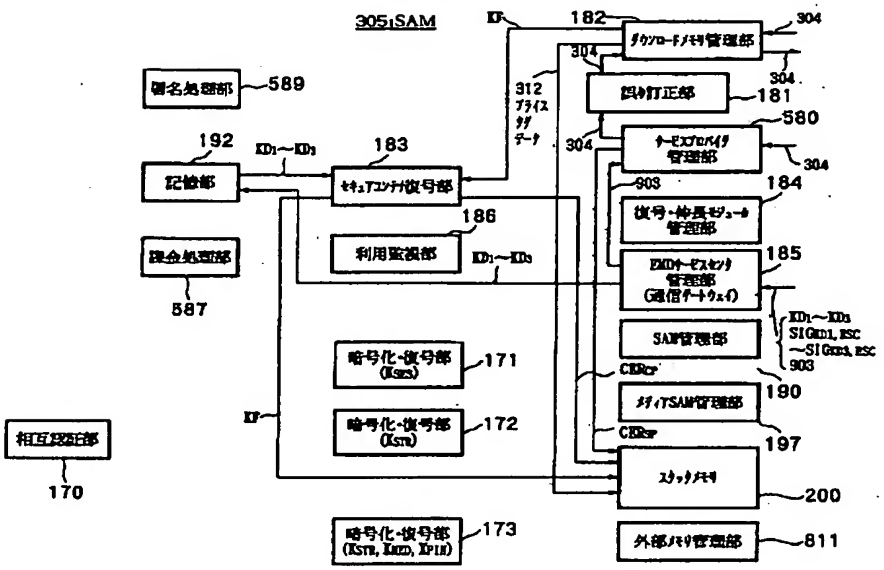
【図５２】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークに配信用鍵データを送信する
S21
EMDサービスセンタは権利書データを登録して権威化する
S22
コンテンツプロバイダからサービスプロバイダにセキュアコンテナに供給
S23
サービスプロバイダにおいて、セキュアコンテナの送信元の正当性を確認する
S24
サービスプロバイダにおいてプライスタグデータを作成し、セキュアコンテナ内にプライスタグデータを格納する
S25
EMDサービスセンタはプライスタグデータを登録して権威化する
S26
サービスプロバイダからCAモジュールにセキュアコンテナを供給
S27
CAモジュールにおいてSP用購入履歴データを作成し、サービスプロバイダに送信する
S28

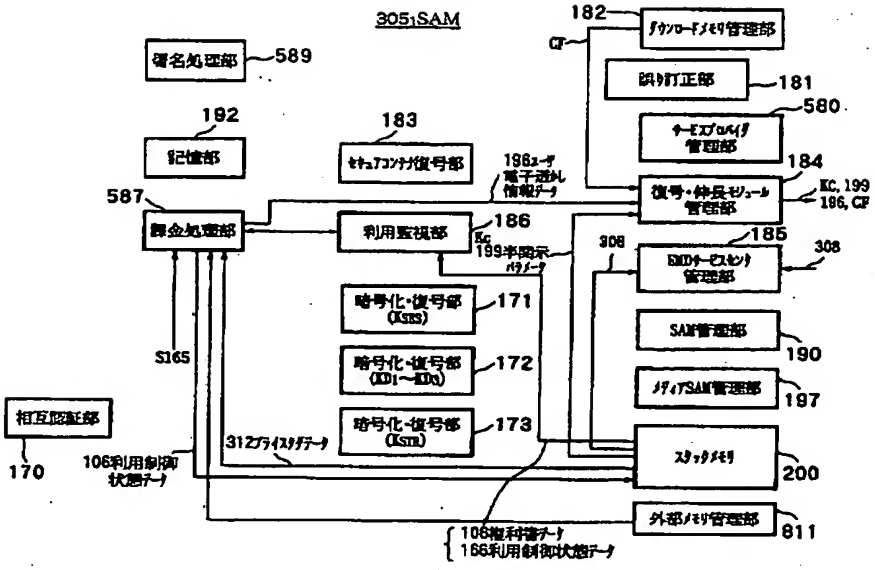
【図４３】


通信記憶モジュール 162
309 SP購入履歴
304 Km, Lr
相互認証部
906
暗号化・復号部
928
復号部
910
912
ICカード
記憶部
907
900
309
911
セキュアコンテナ選択部
SP用購入履歴データ生成部
909
905 復号モジュール
304
311
CAモジュール
166
S65
SAM 905

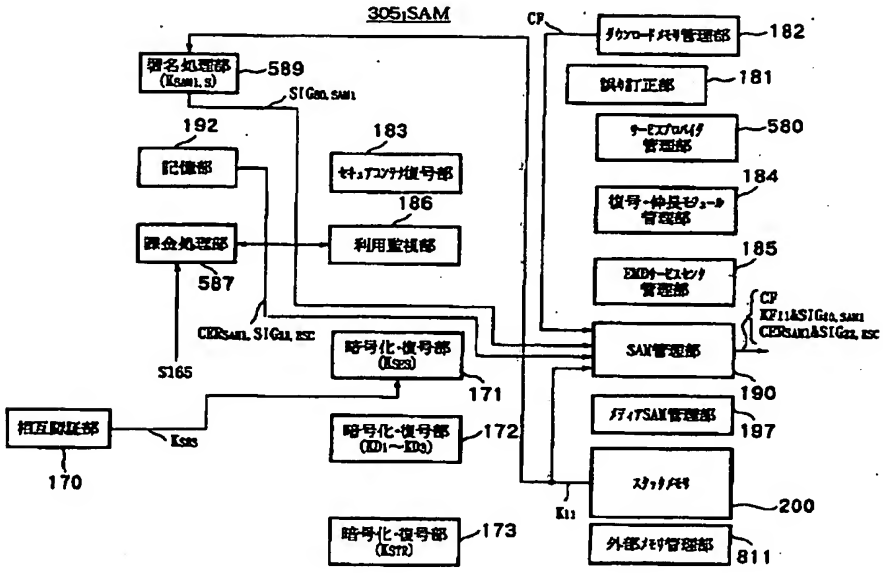
【図４４】


305 SAM
182
304
署名処理部
589
312
181
192
183
580
記憶部
184
186
利用監視部
185
587
171
172
相互認証部
170
190
197
200
173
811
903

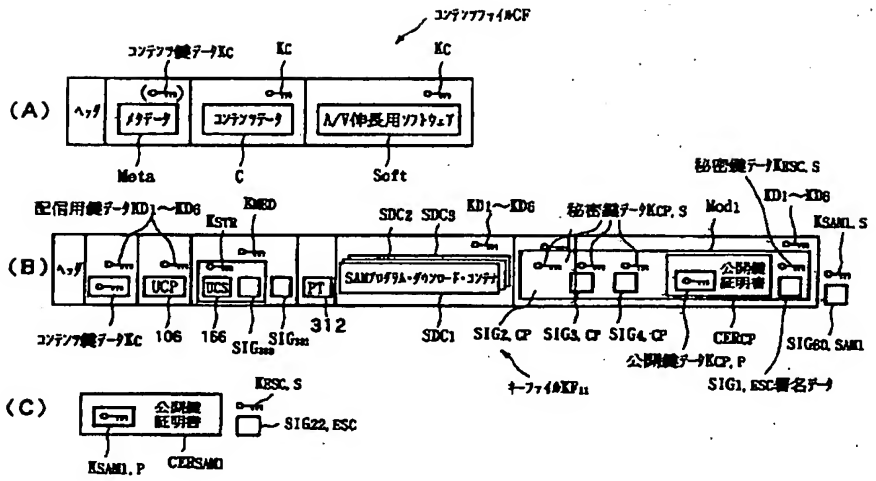
【図４６】


305:SAM
署名処理部
589
182
CF
ダウンロードメモリ管理部
誤り訂正部
181
580
サービスプロバイダ管理部
192
記憶部
183
セキュアコンテナ復号部
198:ユーザ電子透かし情報データ
184
復号・伸長モジュール管理部
KC, 199
196, CF
587
課金処理部
利用監視部
186
Kc
199:半減示パラメータ
308
185
EMDサービスセンタ管理部
308
暗号化・復号部(KSES)
171
S165
暗号化・復号部(KD1～KDn)
172
SAM管理部
190
メディアSAM管理部
197
相互認証部
暗号化・復号部(KSTR)
173
312:プライスリストデータ
スタックメモリ
200
170
106:利用制御状態データ
外部メモリ管理部
811
106:権利書データ
166:利用制御状態データ

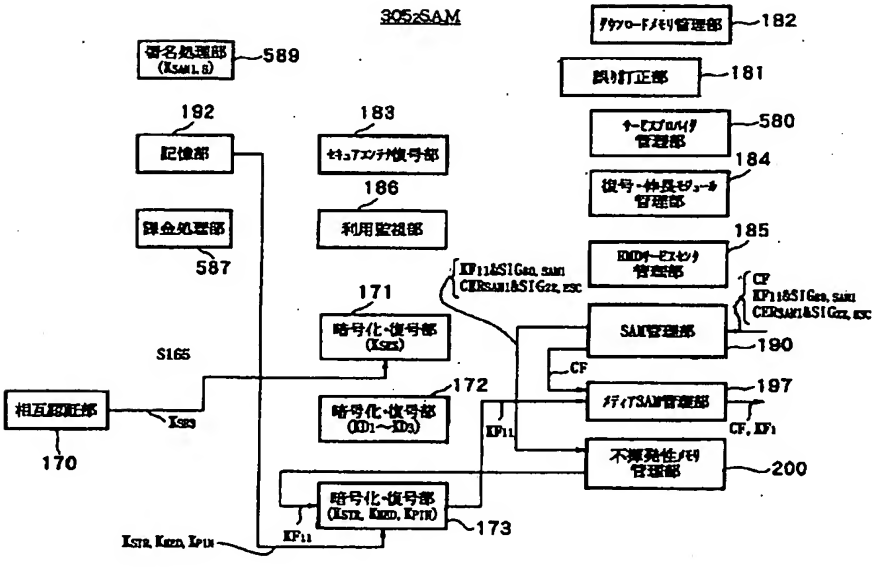
【図４９】


305:SAM
CF
ダウンロードメモリ管理部
182
署名処理部(KSAM1, 3)
589
SIGSAM1
誤り訂正部
181
192
記憶部
183
セキュアコンテナ復号部
サービスプロバイダ管理部
580
186
利用監視部
184
復号・伸長モジュール管理部
課金処理部
587
185
EMDサービスセンタ管理部
CF
KF11&SIGSAM1
CERSAM1&SIGSAM1
CERSAM1, SIGSAM1
暗号化・復号部(KSES)
171
SAM管理部
S165
190
メディアSAM管理部
197
相互認証部
暗号化・復号部(KD1～KDn)
172
KSES
スタックメモリ
200
170
K11
暗号化・復号部(KSTR)
173
外部メモリ管理部
811

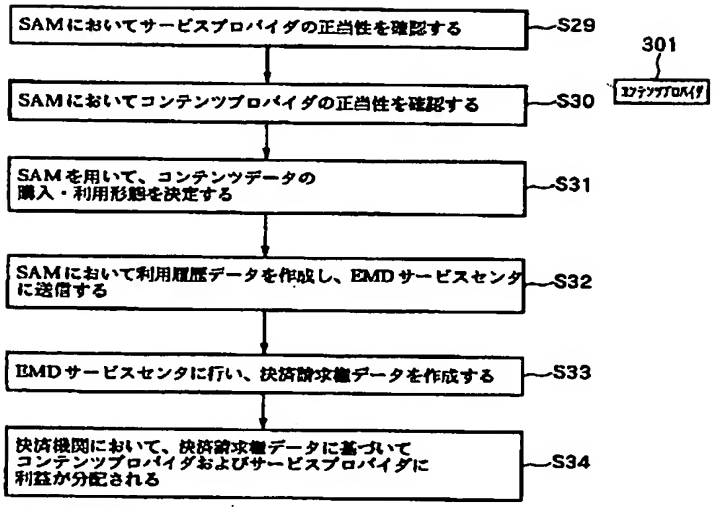
【図５０】


(A)
ヘッダ
メタデータ
コンテンツデータ
A/V伸長用ソフトウェア
Meta
C
Soft
(B)
ヘッダ
UCP
UCS
PT
312
SAMプログラム・ダウンロード・コンテンツ
公開鍵証明書
CERCP
(C)
公開鍵証明書
CERSAM1

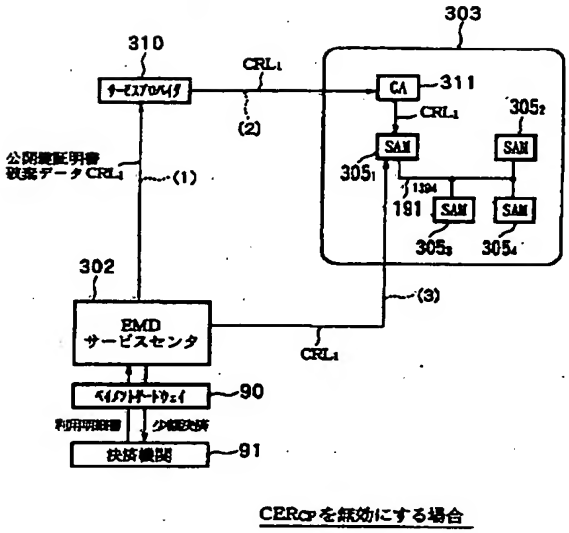
【図５１】


305:SAM
署名処理部
589
ダウンロードメモリ管理部
182
誤り訂正部
181
192
記憶部
183
セキュアコンテンツ復号部
186
利用監視部
課金処理部
587
キープロバイダ管理部
580
184
復号・伸長モジュール管理部
185
RMDサービスセット管理部
CF
KF11&SIG60, SAM1
CERSAM1&SIG22, ESC
171
暗号化・復号部
SAM管理部
190
S165
CF
172
暗号化・復号部
メディアSAM管理部
197
CF, KF1
KF11
相互認証部
KSES
170
不揮発性メモリ管理部
200
暗号化・復号部
173
KF11
KSTR, KMED, KP11

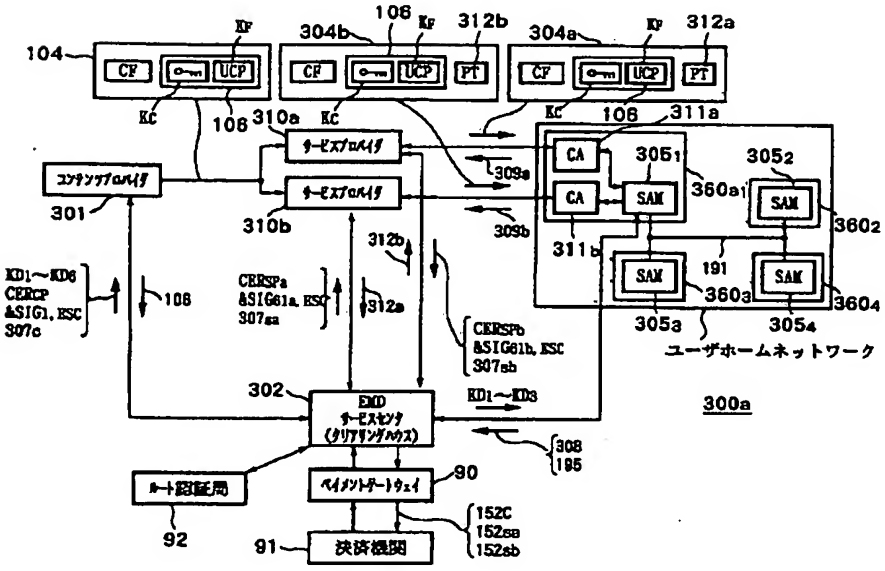
【図５３】


SAMにおいてサービスプロバイダの正当性を確認する
S29
SAMにおいてコンテンツプロバイダの正当性を確認する
S30
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S31
SAMにおいて利用履歴データを作成し、EMDサービスセンタに送信する
S32
EMDサービスセンタにおいて、決済請求書データを作成する
S33
決済機関において、決済請求書データに基づいてコンテンツプロバイダおよびサービスプロバイダに利益が分配される
S34
301
コンテンツプロバイダ

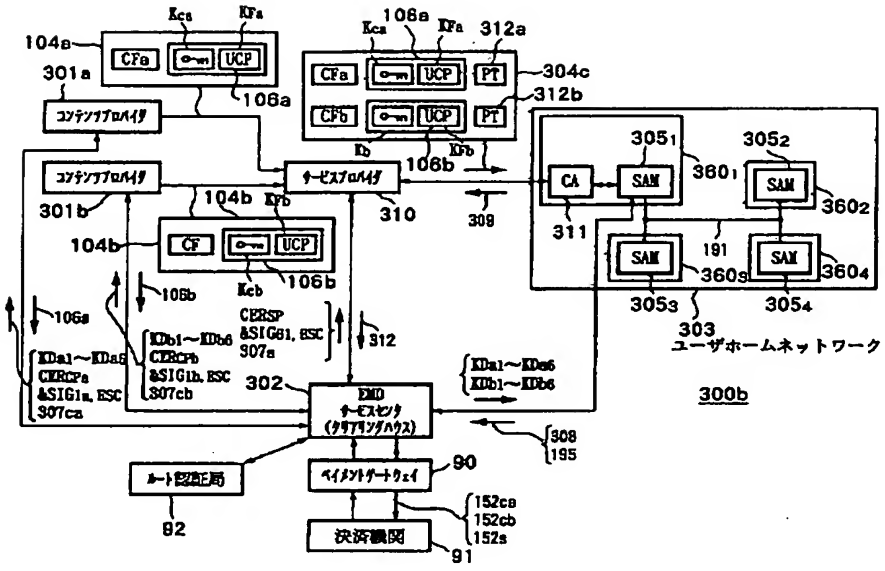
【図５９】


303
310
CRL1
CA
311
CRL1
(2)
公開鍵証明書
改竄データCRL1
(1)
SAM
SAM
SAM
SAM
SAM
1394
191
3051
3052
3053
3054
302
(3)
EMD
サービスセンタ
CRL1
ペイメントゲートウェイ
90
決済機関
91
CERCPを無効にする場合

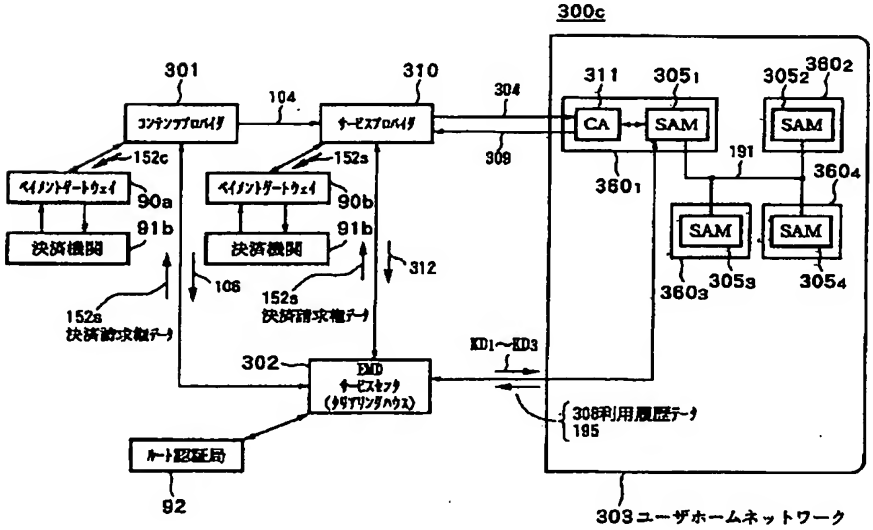
【図５４】


104
CF
KF
UCP
KC
108
304b
106
312b
PT
310a
310b
311a
CA
SAM
3051
3052
3053
3054
360a1
3602
3603
3604
191
311b
309a
309b
301
コンテンツプロバイダ
KD1～KD6
CERCP
&SIG1, KSC
307c
CERSPa
&SIG61a, KSC
307aa
312a
CERSPb
&SIG61b, KSC
307ab
KD1～KD3
302
EMD
サービスセンタ
(クリアリングハウス)
308
195
90
92
91
152C
152ca
152cb
ユーザホームネットワーク
300a

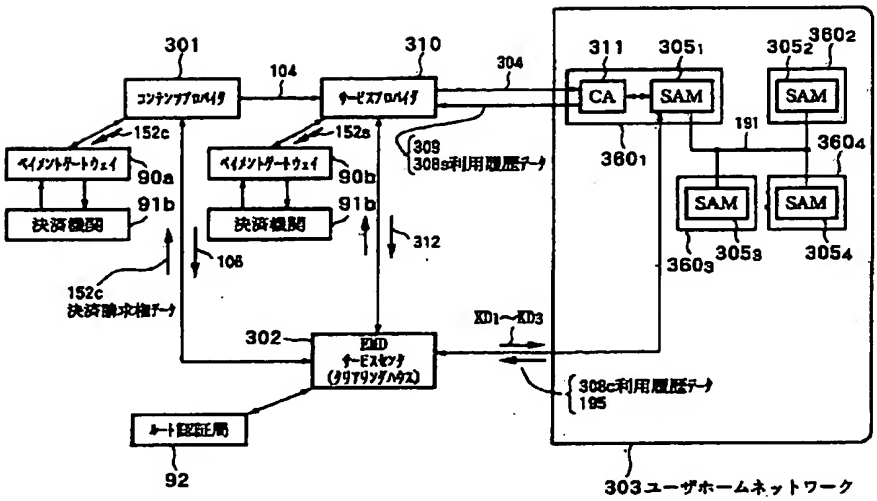
【図５５】


Kcs
KFa
104a
CFa
UCP
301a
106a
108a
312a
304c
312b
PT
CFb
Kb
KFb
106b
3051
3052
360₁
SAM
CA
3602
311
191
3603
3604
3053
3054
303
ユーザホームネットワーク
300b
301b
104b
CF
Kcb
105b
105a
CERSP
&SIG61, ESC
307a
312
KDb1～KDb6
CERCPb
&SIG1b, ESC
307cb
KDa1～KDa6
CERCPa
&SIG1a, ESC
307ca
302
EMD
90
92
91
152ca
152cb
152s
308
195

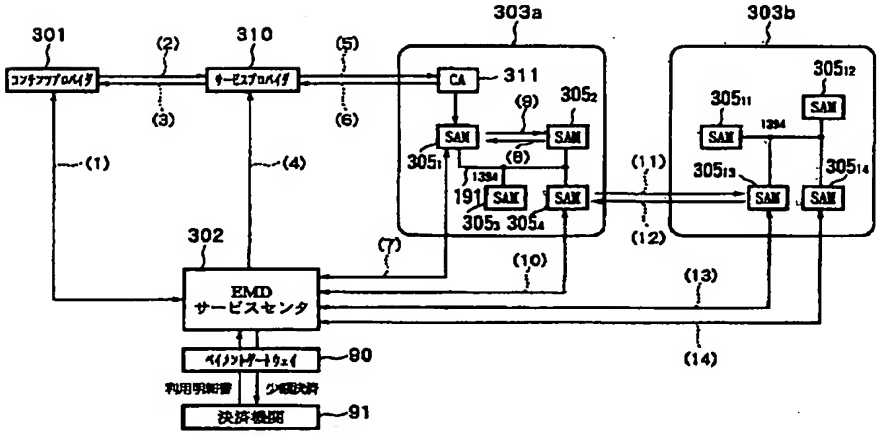
【図５６】


300c
301
310
104
304
311
3051
3052
3602
CA
SAM
309
3601
191
3604
152c
90a
90b
91b
312
106
152s
KD1～KD3
302
EMD
92
308利用履歴データ
195
303ユーザホームネットワーク

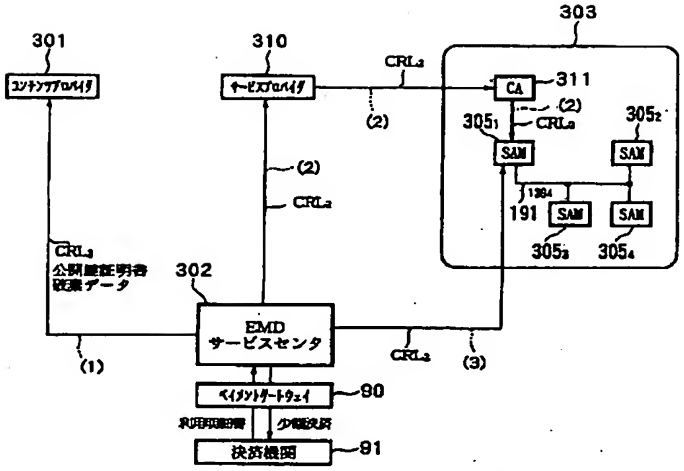
【図５７】


301
310
104
304
311
305₁
3052
3602
CA
SAM
152c
152a
309
308s利用履歴データ
191
3604
90a
90b
91b
91b
3601
312
108
3603
3053
3054
152c
決済請求権データ
302
EMD
サービスセンタ
XD1～XD3
308c利用履歴データ
195
92
303ユーザホームネットワーク

【図５８】

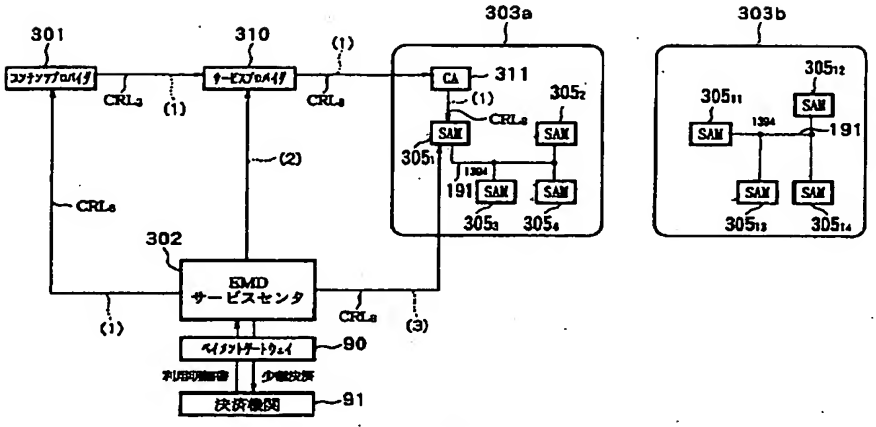

303a
303b
301
310
(2)
(5)
CA
311
(3)
(6)
(9)
305₂
(1)
(4)
(8)
305₁
1394
191
305₃
305₄
(11)
305₁₂
305₁₁
305₁₃
305₁₄
(12)
302
(7)
(10)
(13)
EMD
サービスセンタ
(14)
90
91
公開鍵証明書の入手ルート

【図６０】



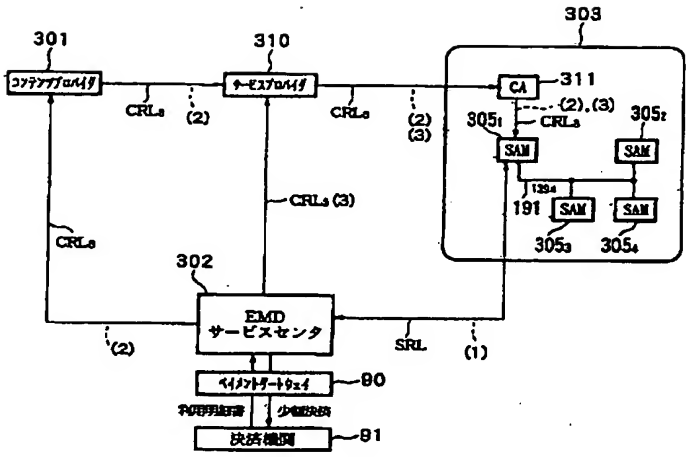
CERSPを無効にする場合

【図６１】

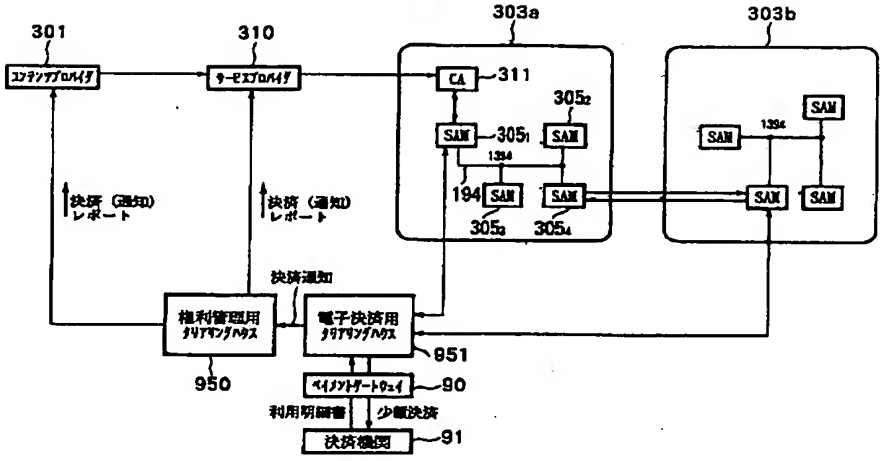


CERSAM2を無効にする場合

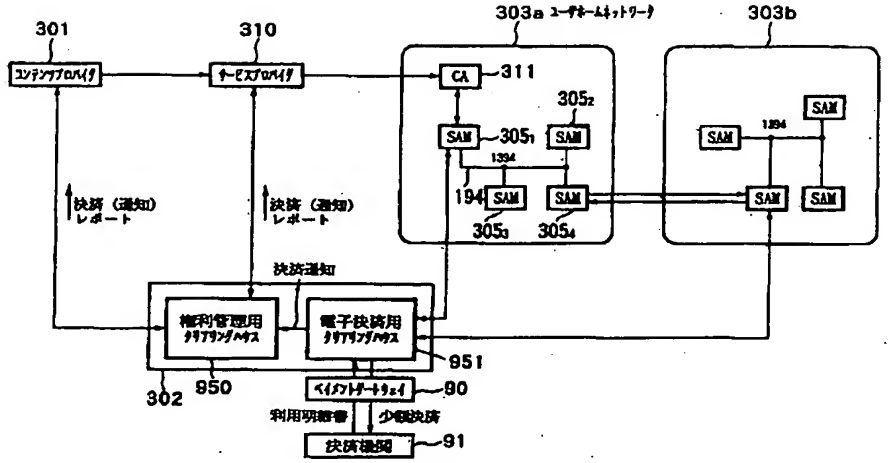
【図６２】


301
310
303
311
CA
SAM
CRLs
(2)
(3)
(2),(3)
CRLs (3)
302
EMD
サービスセンタ
SRL
(1)
90
91
191
1394

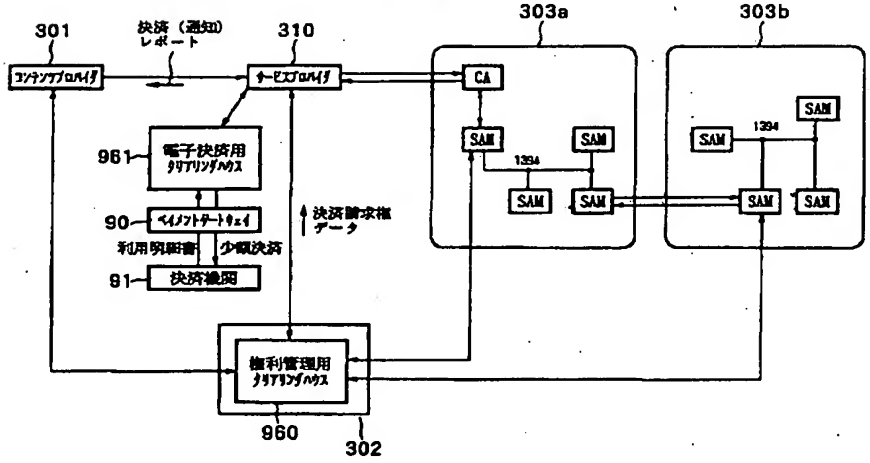
【図６３】


301
310
303a
303b
311
CA
SAM
1394
194
決済（通知）
レポート
決済通知
権利管理用
タリアマンダハウス
電子決済用
タリアマンダハウス
950
951
90
91
利用明細書
少額決済

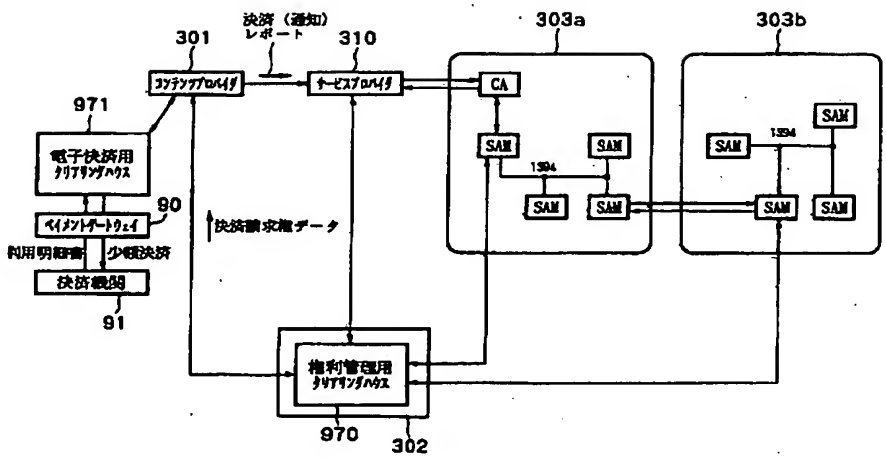
【図６４】


301
310
303a
303b
CA
311
SAM
1394
194
決済（通知）レポート
決済通知
権利管理用
電子決済用
951
950
302
90
91
利用明細書
少額決済
決済機関

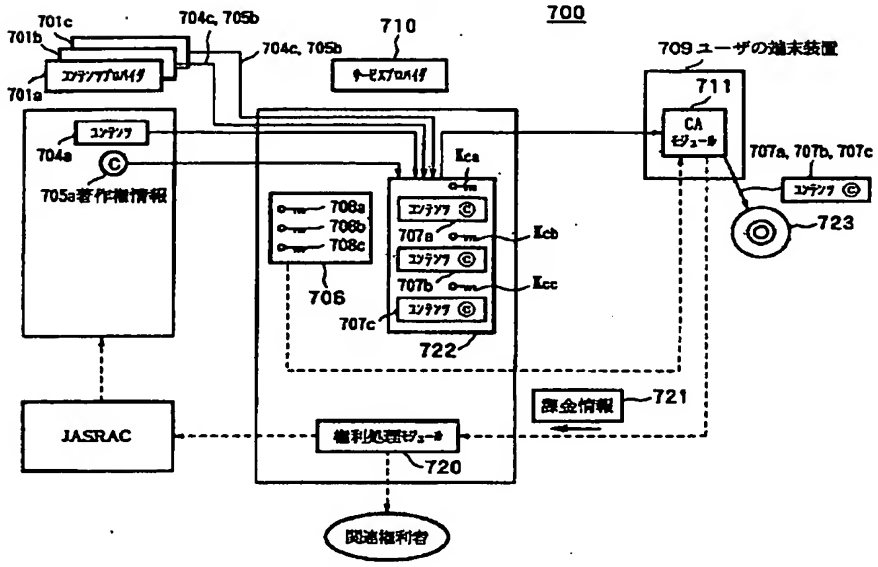
【図６５】


301
決済（通知）レポート
310
303a
303b
CA
SAM
1394
961
電子決済用
90
決済請求額データ
利用明細書
少額決済
91
決済機関
権利管理用
960
302

【図６６】



【図６７】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　15/21	Ｚ	
9/32		Ｈ０４Ｌ　9/00	６０１Ｂ	
			６７５Ｂ	
			６７５Ｄ	

Ｆターム(参考) 5B049 AA05 BB11 BB46 CC05 CC36
DD05 EE03 EE05 EE59 FF09
GG04 GG07 GG10
5B089 GA11 GA21 GB04 HA10 JB22
KA15 KA17 KB13 KC58
5D044 AB05 DE48 GK12 GK17 HL11
5J104 AA07 AA09 AA14 KA01 LA03
LA06 MA02 PA07
9A001 CC02 EE03 EE04 HH15 KK43
LL03